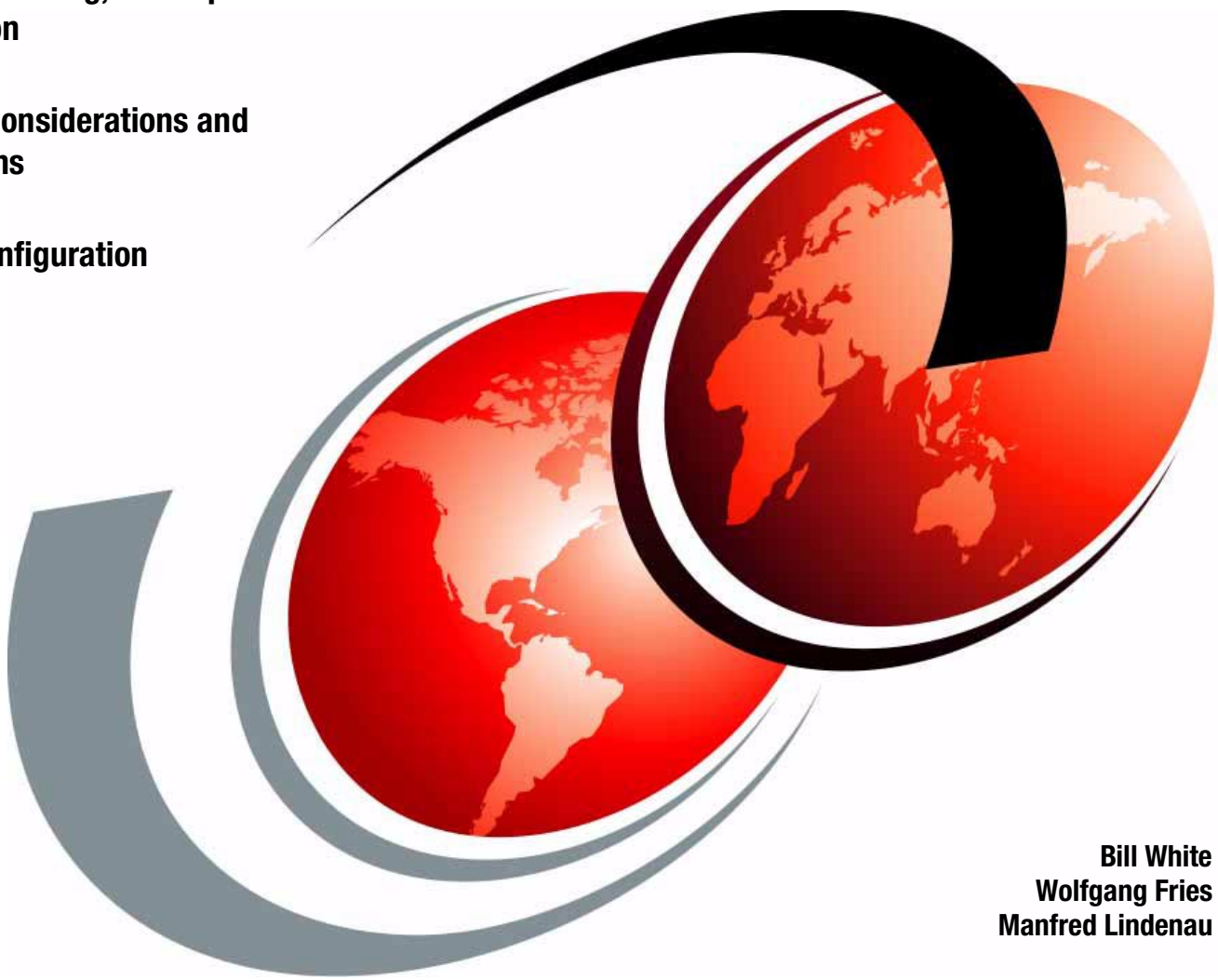
IBM

Getting Started with the McDATA Intrepid FICON Director

- Product, planning, and implementation information
- Realistic considerations and suggestions
- Helpful configuration examples



Bill White
Wolfgang Fries
Manfred Lindenau

Redbooks

ibm.com/redbooks

International Technical Support Organization

Getting Started with the McDATA Intrepid FICON Director

April 2003

SG24-6857-00

Note: Before using this information and the product it supports, read the information in “Notices” on page v.

First Edition (April 2003)

This edition applies to firmware version 4.1.0 (Build 12) of McDATA Intrepid FICON Director.

© Copyright International Business Machines Corporation 2003. All rights reserved.
Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices v
Trademarks vi

Preface vii
The team that wrote this redbook. vii
Become a published author viii
Comments welcome. viii

Chapter 1. Introduction 1
1.1 Basic Fibre Channel terminology 2
1.2 FICON overview 4
1.2.1 FICON channel architecture 4
1.2.2 FICON channel support 5
1.3 FICON channel topology. 6
1.3.1 Switched point-to-point configuration 6
1.3.2 Cascaded FICON Director configuration. 8

Chapter 2. Technical description 11
2.1 Introduction to the FICON Director 12
2.1.1 FICON Director overview 12
2.1.2 Management capabilities 13
2.1.3 EFC Server hardware requirements 14
2.1.4 Hardware components 15
2.1.5 FICON Director configurations 17
2.1.6 FICON SANtegrity feature. 18
2.1.7 Control Unit Port (CUP). 19

Chapter 3. Pre-installation planning 21
3.1 Planning recommendations. 22
3.2 Physical port layout 23
3.3 IP addressing and connectivity 23
3.4 Switch numbering 25
3.5 Binding and Insistent Domain ID. 28
3.6 Zoning 30
3.7 Cables and connectors 31
3.8 FICON channel support for zSeries and 9672 G5/G6 servers 32
3.8.1 FICON channel distances 33
3.8.2 FICON channel to control unit characteristics. 34

Chapter 4. Setting up the EFC Server environment 35
4.1 Installation and setup 36
4.2 Usage options 38
4.2.1 Products 38
4.2.2 Fabrics 40
4.2.3 Users. 41
4.2.4 Logs 41

Chapter 5. Configuring the FICON Director 45
5.1 Setting up a FICON Director 46

© Copyright IBM Corp. 2003. All rights reserved.

5.2 Activating the High Integrity feature 48
5.3 Enabling the Control Unit Port (CUP) 50
5.4 Building a fabric. 52
5.4.1 Switch Binding 56
5.5 Port configuration 58
5.5.1 Defining Nicknames 58
5.5.2 Defining port names and blocking ports 59
5.5.3 Configuring a port 61
5.6 Zoning 61
5.6.1 Creating a zone. 62
5.6.2 Creating a zone set. 63
5.6.3 Activating a zone set. 65
5.7 Verifying and backing up the configuration 68

Appendix A. Useful procedures. 71
Setting up a HyperTerminal session 72
Altering an IP address in a CTP card. 74
Installing EFC Manager server software 75
Installing EFC Management client software. 76
Upgrading Director firmware 76

Appendix B. Port location and mapping. 79
Intrepid port numbering 80
Intrepid 6064 port address mapping 80
Intrepid 6140 port address mapping 81

Appendix C. FICON Director configuration worksheet 85

Related publications 87
IBM Redbooks 87
Other resources 87
Referenced Web sites. 87
How to get IBM Redbooks 87
IBM Redbooks collections. 87

Index 89

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:
This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

© Copyright IBM Corp. 2003. All rights reserved.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

ESCON®
FICON™
IBM®
IBM eServer™
OS/390®
Perform™
Redbooks™
Redbooks(logo)™
S/390®
SP™
Wave®
z/OS™
zSeries™
Lotus®
Word Pro®

The following terms are trademarks of other companies:

ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

C-bus is a trademark of Corollary, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

SET, SET Secure Electronic Transaction, and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

Other company, product, and service names may be trademarks or service marks of others.

Preface

This IBM Redbook discusses how to install, tailor, and configure the McDATA Intrepid FICON Director, in conjunction with the FICON topologies supported by zSeries and 9672 Generation 5 and Generation 6 servers. It focuses on the hardware installation as well as the software definitions needed to provide connectivity for supported FICON environments.

This redbook provides planning information and FICON Director setup information. Also included are helpful utilities for monitoring and managing the McDATA Intrepid FICON Director environment.

This document is intended for system engineers, SAN administrators, and system programmers who will plan and install McDATA Intrepid FICON Directors. A good background in systems planning, hardware and cabling infrastructure planning, and zSeries I/O definitions (HCD or IOCP), as well as Fibre Channel or FICON Directors is assumed.

The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization, Poughkeepsie Center.

Bill White is a Project Leader and Senior Networking Specialist at the International Technical Support Organization, Poughkeepsie Center.

Wolfgang Fries is a Senior Consultant in the zSeries Support Center in Germany. He has 25 years of experience in supporting large zSeries and S/390 customers. His area of expertise include zSeries servers and connectivity.

Manfred Lindenau is a S/390 and zSeries specialist in Germany. He has 23 years of experience in IBM Large Systems Technical Support and currently works in the German Support Center in Mainz. His areas of expertise include S/390 and zSeries channel subsystems and Parallel, ESCON, and FICON interfaces.

Thanks to the following people for their contributions to this project:

Robert Haimowitz
International Technical Support Organization, Raleigh Center

Dan Elmendorf
IBM zSeries Planning

Charles Hubert
Brian Jacobs
IBM FICON Development

Ron Peck
IBM FICON Director Program Manager

Dean Armand, Neal Fausett, Guy McConnell, Jesus Perez, Barbara Sewell, Larry Shane
McDATA Corporation

© Copyright IBM Corp. 2003. All rights reserved.

Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You'll team with IBM technical professionals, Business Partners and/or customers.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you'll develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our Redbooks to be as helpful as possible. Send us your comments about this or other Redbooks in one of the following ways:

- Use the online **Contact us** review redbook form found at:

  ibm.com/redbooks

- Send your comments in an Internet note to:

  redbook@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. HYJ Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

1

Introduction

McDATA Intrepid FICON Directors are a product of a reseller agreement between IBM and McDATA Corporation. They are designed to provide enterprise-class availability and Fibre Channel connectivity for IBM servers and storage products supporting Fibre Channel (FC) and FICON protocols.

The intent of this chapter is to provide background information about the zSeries FICON environment in which McDATA Intrepid FICON Directors are deployed. In the subsequent sections, you will find the following:

- Basic FICON and Fibre Channel terms
- FICON overview
  - FICON channel support
- Supported FICON Director topologies:
  - Switched point-to-point
  - Cascaded FICON Directors
  - High integrity

© Copyright IBM Corp. 2003. All rights reserved.

1.1 Basic Fibre Channel terminology

This section discusses some general terms used in the Fibre Channel (FC) environment. These terms are also used in FICON environments when installing, configuring, and operating in a switched point-to-point or cascaded FICON Director configuration, therefore, you will find these terms throughout this document.

Node

A node is an endpoint that contains or uses information. It can be a computer (host), a device controller, or a peripheral device (such as disk or tape drives). A node has a unique 64-bit identifier known as the Node_Name. The Node_Name is typically used for management purposes.

Port

Each node must have at least one port (hardware interface) to connect the node to the FC topology. This node port is referred to as an N_Port.

Each N_Port has a Port_Name which is a unique 64-bit identifier that is assigned when it is manufactured. The N_Port associates an access point to a node's resources.

Other port types present in an FICON switched environment include:

E_Port An *expansion port* is used to interconnect switches and build a switched fabric.
F_Port A *fabric port* is used to connect a N_Port to a switch that is not loop-capable.
G_Port A *generic port* is a port that has not assumed a role in the fabric.

Switched fabric

One or more FC switches (FC-SW) can be interconnected to create a fabric, to which N_Ports are connected. A switched fabric takes advantage of aggregated bandwidth via switched connections between N_Ports using *packet-switching*. FC switches (FICON Directors) allow multiple concurrent I/O operations (read and write) between multiple FICON-capable servers and multiple FICON-capable control units (devices).

FC link

The port connects to the topology through an FC link (see Figure 1-1). The transmission medium for the FC link (FICON interface) is a fiber optic cable. Physically, it is a pair of optical fibers that provide two dedicated, unidirectional, serial-bit transmission lines. Information in a single optical fiber flows, bit by bit, and always in the same direction. At any link interface, one optical fiber is used to receive data while the other is used to transmit data. Full duplex capabilities are exploited for data transfer. The Fibre Channel Standard (FCS) specifies that for normal I/O operations, frames flow serially in both directions, allowing several concurrent read and write I/O operations on the same link.

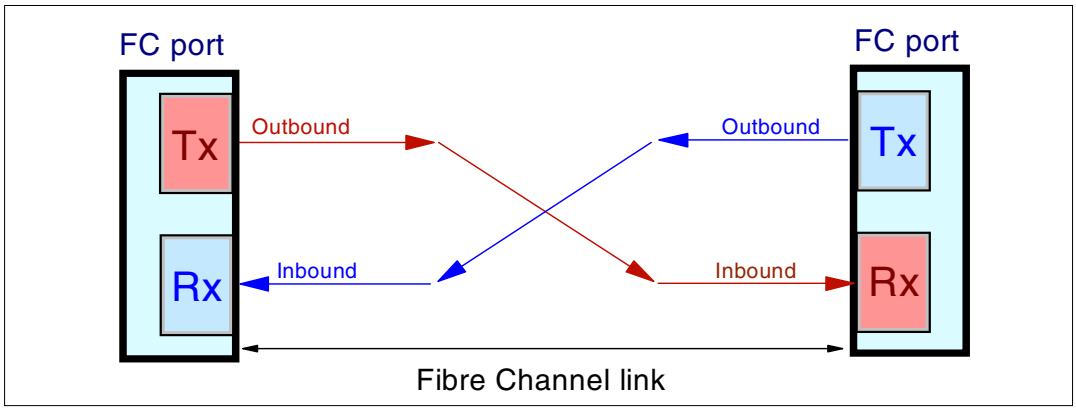


Figure 1-1 Fibre Channel Link

An FC link (port-to-port connection) can be:

- Node-to-node (N_Port-to-N_Port)
- Node-to-switch (N_Port-to-F_Port)
- Switch-to-switch (E_Port-to-E_Port)

The FC link data rate is 1 Gbps (100 MBps) for zSeries and 9672 G5/G6 FICON feature ports, and 1 Gbps or 2 Gbps (200 MBps) for zSeries FICON Express feature ports. The 2 Gbps link capability is auto-negotiated between the zSeries server and FICON Director, as well as the Director and devices, and is transparent to the operating system and application. With devices in general, the zSeries FICON Express, FICON Director, and/or device communicate and agree upon either a 1 Gbps or 2 Gbps (100 MBps or 200 MBps) link speed. This speed determination is based upon the adapter speeds in the zSeries server, FICON Director, and device, as well as the fiber optic cable infrastructure capabilities. For those parts of the I/O infrastructure that are not 2 Gbps link-capable, the link speed will be auto-negotiated to 1 Gbps (100 MBps).

Note: The 2 Gbps line speed is the theoretical maximum unidirectional bandwidth capability of the fiber link. The actual throughput potential of the 2 Gbps link (whether it is measured in I/O operations per second, or MBps) will depend on the type of workload, fiber infrastructure, and storage devices in place.

World-Wide Names (WWN)

As mentioned, nodes and ports have unique 64-bit addresses that identify them in an FC or FICON topology. These addresses are assigned by the manufacturer, with a vendor-specific portion defined by the IEEE standards committee. These addresses (in the FC standard) are called Node_Names and Port_Names, and when they are world-wide unique, they are referred to as:

- World-Wide Node_Name (WWNN)
- World-Wide Port_Name (WWPN)

A WWN (any WWNN or WWPN) is usually written in sets of two hex digits, separated by colons (for example, 08:45:12:56:43:00:D5:A0). Figure 1-2 illustrates the use of WWNs.

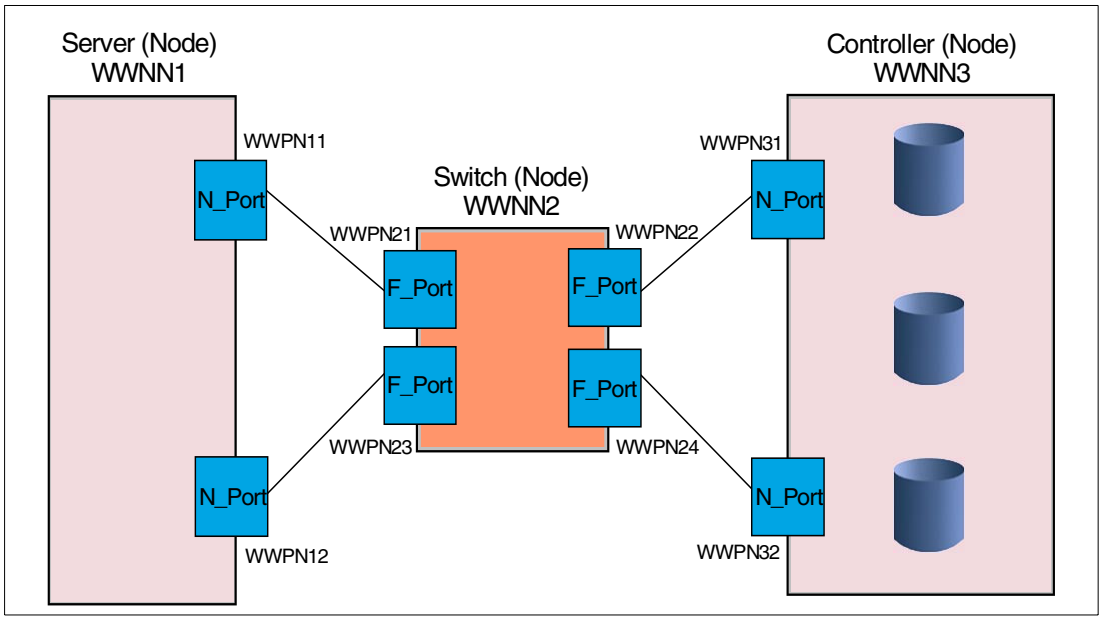


Figure 1-2 Example of World-Wide Names

1.2 FICON overview

There are a number of characteristics and functional areas that need to be understood in designing an I/O configuration that exploits FICON technology. This section introduces the basics of these areas for the FICON channel.

1.2.1 FICON channel architecture

The FICON channel architecture consists of the following Fibre Channel (FC) protocols:

- FC-0 level: Interface and Media

  The Fibre Channel physical interface (FC-0), specified in FC-PI, consists of the transmission media, transmitters, receivers, and their interfaces. The physical interface specifies a variety of media and associated drivers and receivers capable of operating at various speeds.

  ANSI NCITS xxx-200x FC-PI T11/Project 1235D

- FC-1 level: Transmission Protocol

  This is a link control protocol that performs a conversion from the 8-bit EBCDIC code into a 10-bit transmission code; a unique bit-pattern is assigned to each known hexadecimal character. Encoding is done by the N_Port when sending the character stream over the fiber and decoding back to 8-bit code is performed by the receiving N_Port.

- FC-2 level: Signaling Protocol

  Fibre Channel physical framing and signaling interface (FC-PH) describes the point-to-point physical interface, transmission protocol, and signaling protocol of high-performance serial links for support of higher-level protocols associated with HIPPI, IPI, SCSI, FC-SB2 (FICON) and others.

  – Fibre Channel - Framing and Signalling (FC-FS)

    ANSI X3.230-1994

Describes the signaling protocol of the high-performance serial link for support of higher-level protocols associated with HIPPI, IPI, FC-FCP (SCSI), FC-SB2 (FICON) and others.

This architecture covers the Fibre Channel levels FC-1, FC-2, and some parts of the FC-3 level.

The FC-FS architecture consolidates the relevant clauses of FC-PH (the initial Fibre Channel architecture), its amendments 1 and 3, and FC-PH-2 and FC-PH-3 protocols, but does not replace those protocols. In this redbook the FC-FS architecture is referred to as the zSeries and 9672 G5/G6 processors, which comply with the FC-FS functions. These functions are described in more detail in the FC-FS architecture.

- FC-3 level: Common Services

  This level is reserved for future functions.

- FC-4 level: Mapping

  Channels Upper Level Protocol (ULP) as part of FC-4 and describes IPI/FC-FCP (SCSI)/ HIPPI/SB/IP and FC-SB-2 (FICON) protocols.

  Other standards used in the Fibre Channel architecture, and their references:

  – Fibre Channel - Switch Fabric (FC-SW)

    ANSI X3T11/Project 959-D/Rev 3.3

  – Single-Byte Command Code Sets Connection Architecture (SBCON)

    ANSI X3.296-199x

  – Fibre Channel Fabric Generic Requirements (FC-FG)

    Describes minimum requirements for a topology-independent interconnecting fabric to support FC-PH.

    ANSI X3.289-199x

  – Fibre Channel Switch Fabric (FC-SW)

    Specifies tools and algorithms for interconnection and initialization of FC switches to create a multi-switch Fibre Channel Fabric.

    ANSI X3T11/Project 959-D/Rev 3.3

  FC-SB-2 (FICON) architecture information and all other documentation mentioned can be obtained from the following Web site:

  http://www.t11.org

1.2.2 FICON channel support

FICON channel support in the zSeries and 9672 G5/G6 servers can operate in one of three modes:

- A FICON channel in FICON Bridge (FCV*)* mode allows access to ESCON control units with ESCON interfaces by the channel connected to a FICON Bridge adapter in a 9032-5 ESCON Director. This mode is applicable only to the FICON LX features.
- A FICON channel in FICON native (FC*)* mode allows access to FICON native interface control units either directly by a FICON channel in FC mode (point-to-point), or from a FICON channel in FC mode connected in series through one or two Fibre Channel switches (FICON Directors). Channel-to-channel (FCTC) is also supported in this mode.

Note: The 9672 G5/G6 processors only support a single switch topology, known as switched point-to-point, whereas, the zSeries processors support single and dual switch topologies. A two-switch configuration is known as cascaded FICON Directors.

- A FICON channel in Fibre Channel Protocol (FCP) mode can access FCP devices in one of two ways:
  - Through a FICON channel in FCP mode through a single Fibre Channel switch or multiple switches to an FCP device
  - Through a FICON channel in FCP mode through a single Fibre Channel switch or multiple switches to a Fibre Channel-to-SCSI bridge

Note: The 9672 G5/G6 processors *do not* support FICON channels in FCP mode. Point-to-point and arbitrated loop topologies *are not* supported as part of the zSeries FCP enablement. This mode is only supported in conjunction with Linux environments.

1.3 FICON channel topology

A FICON channel in FICON native (FC) mode uses the Fibre Channel communication infrastructure supported by the zSeries and 9672 G5/G6 servers to transfer channel programs (CCWs) and data via its FICON and FICON Express features to another FICON-capable node, such as a storage device, printer or server (channel-to-channel).

A FICON channel (in conjunction with the McDATA FICON Director) can operate in two topologies:

- Switched point-to-point (through a single FICON Director to FICON-capable control units)
- Cascaded FICON Directors (through two FICON Directors to FICON-capable control units)

The FICON channel in FICON native (FC) mode supports multiple concurrent I/O connections. Each concurrent I/O operation can be to the same FICON control unit (but to different devices/CU images), or to different FICON control units.

1.3.1 Switched point-to-point configuration

In a switched point-to-point connection, at least two Fibre Channel (FC) links are needed in the channel-control unit path. One is between the FICON channel card (N_Port) and the FICON Director port (F_Port), then internally within the switch (through the backplane) to another port (F_Port) and then via the second link to a FICON adapter card in the control unit (N_Port).

The FICON channel determines whether the associated link is in a point-to-point or switched topology. It does this by logging into the fabric, fabric login (FLOGI ELS), and checking the accept response to the fabric login (ACC ELS). The FLOGI-ACC (accept) response indicates if the channel N_Port is connected to another N_Port (point-to-point) or an F_Port (fabric port).

An example of a switched point-to-point topology is shown in Figure 1-3.

Multiple channel images and multiple control unit images can share the resources of the Fibre Channel link and the Fibre Channel switch, such that multiplexed I/O operations can be performed.

Channels and control unit links can be attached to the Fibre Channel switch in any combination, depending on configuration requirements and available resources in the Fibre Channel switch.

Sharing a control unit through a Fibre Channel switch means that communication from a number of channels to the control unit can take place over one switch to CU link (in the case where a control unit has only one link to the Fibre Channel switch), or over multiple link interfaces (in the case where a control unit has more than one link to the Fibre Channel switch).

Just one Fibre Channel link is attached to a FICON channel in a FICON switched point-to-point configuration, but from the FC switch (FICON Director) that FICON channel can communicate with a number of FICON CUs on different FC switch ports. Once at the control unit, the same control unit and device addressing capability exists as for a point-to-point configuration. However, the communication and addressing capability is increased for the channel when the channel is connected to a FC switch with the ability to use the domain and port address portion of the 24-bit N_Port address (8 bits for the domain and 8 bits for the port) to access multiple control units.

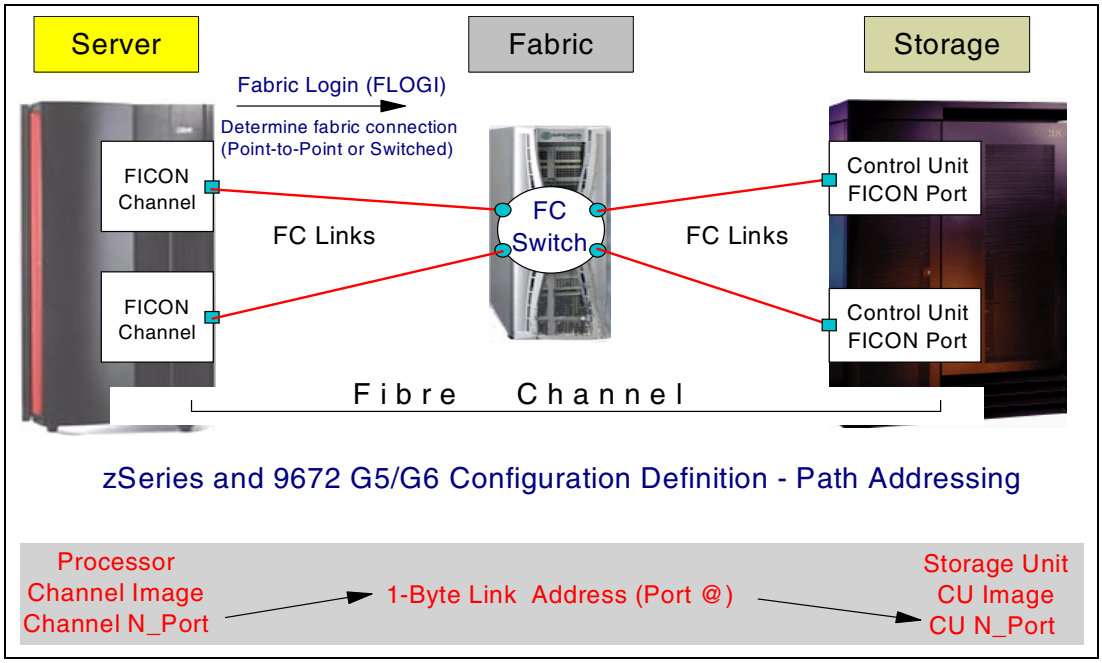


Figure 1-3 Switched point-to-point configuration

The communication path between a channel and a control unit is composed of two different parts: the physical channel path and the logical path.

In a FICON switched point-to-point topology (with a single switch) the physical paths are the FC links, or interconnection of two FC links connected by a FC switch that provides the physical transmission path between a channel and a control unit.

A FICON (FC-SB-2) logical path is the relationship established between a channel image and a control unit image for communication during execution of an I/O operation and presentation of status.

1.3.2 Cascaded FICON Director configuration

In a cascaded FICON Director connection, at least three Fibre Channel (FC) links are needed in the channel-control unit path. One is between the FICON channel card (N_Port) and the FICON Director port (F_Port), then internally within the switch (through the backplane) to another port (E_Port) that connects to the second FICON Director E_Port via the second FC link, and then to a FICON adapter card in the control unit (N_Port) via the third FC link. With this configuration, the connection between sites can consist of multiple FC links.

An example of cascaded FICON Directors is shown in Figure 1-4.

Multiple channel images and multiple control unit images can share resources of the Fibre Channel link and Fibre Channel switches, such that multiplexed I/O operations can be performed.

Channels and control unit links can be attached to the Fibre Channel switches in any combination, depending on configuration requirements and on available switch ports.

Sharing a control unit through a Fibre Channel switch means that communication from a number of channels to the control unit can take place either over one switch-to-CU link (in the case where a control unit has only one link to the Fibre Channel switch), or over multiple link interfaces in the case where a control unit has more than one link to the Fibre Channel switch.

Just one Fibre Channel link is attached to a FICON channel in a cascaded FICON Director configuration. However, from the FC switch (FICON Director) the FICON channel can communicate with a number of FICON CUs on different ports of the second FC switch. Once at the control unit, the same control unit and device addressing capability exists as for a point-to-point configuration. However, the communication and addressing capability is greatly increased for the channel when connected to a FC switch with the ability to use the domain and port address portion of the 24-bit N_Port address (8 bits for the domain and 8 bits for the port) to access multiple control units. Note the domain address portion of the FC 24-bit port address is different since there are two FC switches in the channel-to-control unit path.

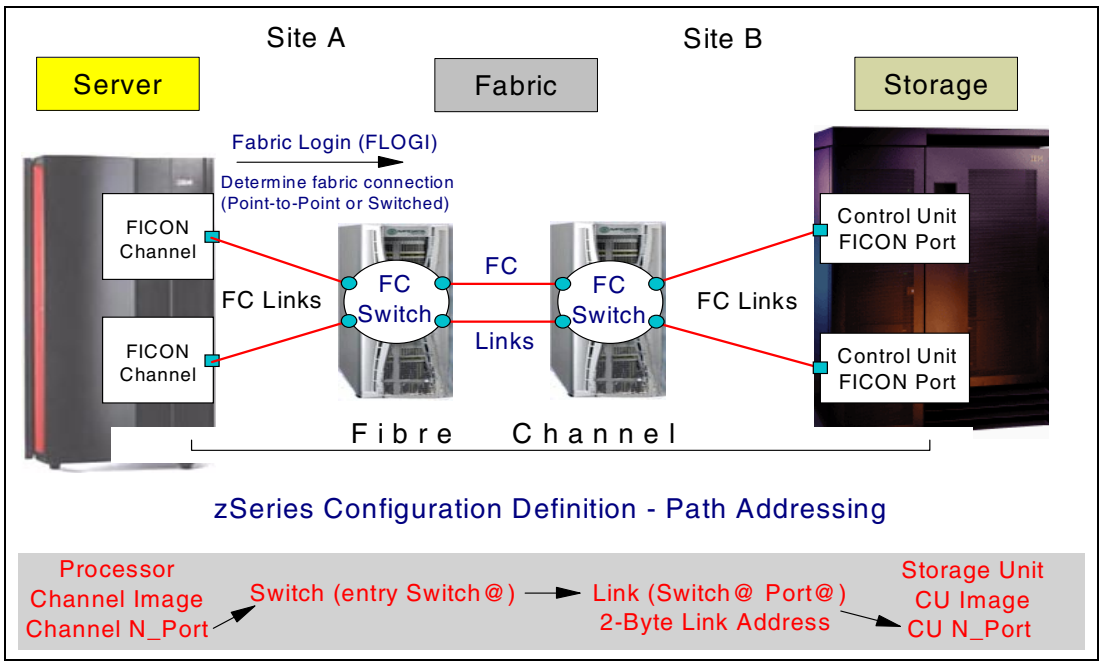


Figure 1-4 Cascaded FICON Directors configuration

The communication path between a channel and a control unit is composed of two different parts, the physical channel path and the logical path.

In a cascaded FICON Director topology, the physical paths are the FC links that provide the physical transmission path between a FICON channel and a control unit.

A FICON (FC-SB-2) logical path is the relationship established between a FICON channel image and a control unit image for communication during execution of an I/O operation and presentation of status.

Note: The cascaded FICON Director configuration is only supported by the zSeries (z800 and z900) servers.

High-integrity data path

Another important value of FICON support of cascaded Directors is its ability to provide high-integrity data paths. The high integrity function is an integral component of the FICON architecture when configuring FICON channel paths through a cascaded fabric.

To support the introduction of FICON cascaded switching, IBM has worked with McDATA to ensure robustness in the channel-to-control unit path is maintained to the same high standard of error detection, recovery, and data integrity that has existed for many years with both ESCON and the initial implementation of FICON.

End-to-end data integrity is designed to be maintained through the cascaded Director fabric. Data integrity ensures any changes to the customer's data streams are always detected, and the data frames (data streams) are delivered to the correct end point; an end point being a FICON channel port or a FICON Control Unit port. For FICON channels, Cyclical Redundancy Checking (CRC) and Longitudinal Redundancy Checking (LRC) are bit patterns added to the customer data streams to allow for detection of any bit changes in the data stream. With FICON support of cascaded switching, new integrity features are introduced within the FICON channel and the FICON cascaded switch fabric to ensure detection and reporting of any miscabling actions occurring within the fabric during operational use that may cause a frame to be delivered to the wrong end point.

A FICON channel, when configured to operate with a cascaded switch fabric, requires the switch fabric supports high integrity. During initialization, the FICON channel queries the switch fabric to determine that it supports high integrity. If it does, the channel completes the initialization process, allowing the channel to operate with the fabric.

Once a FICON switched fabric is customized to support FICON cascaded Directors and the required World-Wide Node Name (WWNN) and Domain IDs have been added in the fabric membership list, the Director checks that its Inter-Switch Links (ISLs) are attached to the correct Director before they are made operational. If an accidental cable swap occurs, the Director invokes logical path testing, reporting, isolation, and recovery. The high-integrity fabric feature for cascaded FICON Directors protects against mis-cabling and mis-directing of data streams.

High-integrity fabric architecture support includes:

- Fabric binding support

  The ability of the fabric to prevent a switch from being added to the fabric that is not configured to support the “high integrity fabric”; for example, all switches must be defined to all other switches via a fabric membership list.

- Insistent Domain IDs support

This support will not allow a switch address to be automatically changed when a duplicate switch address is added to the enterprise fabric. It requires overt operator action to change a switch address.

Note: FICON Directors in a cascaded configuration require the High-Integrity feature .

For more detailed information about FICON planning, implementation, and architecture, refer to *FICON Native Implementation and Reference Guide,* SG24-6266.

2

Technical description

This chapter provides a technical description for the McDATA Intrepid FICON Directors; included are:

- McDATA Intrepid FICON Director overview
- Hardware components
- Model configurations
- Software features:
  - Enterprise Fabric Connectivity Manager
  - High Integrity feature
  - Control Unit Port

© Copyright IBM Corp. 2003. All rights reserved.

2.1 Introduction to the FICON Director

This section provides an overview of the McDATA Intrepid FICON Directors and discusses the hardware components, models, configuration, and software.

2.1.1 FICON Director overview

The McDATA Intrepid models implement Fibre Channel technology that provides high-performance scalable bandwidth, high available operation, and redundant switched data paths that support FICON-attached servers and storage devices.

The Intrepid 6064 FICON Director is an enterprise class Director that provides switch fabric connectivity for to up 64 ports. The Intrepid 6140 is the newest addition and provides up to 140 ports.

Both models have the following characteristics:

- Scalable design
- Automatic failover of critical components
- Based on a Serial Crossbar (SBAR) switching element
- Low latency, non-blocking architecture
- Consistent latency of 2 microseconds
- Software based zoning

The Directors provide a modular design that enables quick removal and replacement of Field Replacable Units (FRUs), including a:

- Cable management assembly and front bezel
- Power module assembly (with AC power switch), redundant fan modules and redundant power supplies
- Redundant processor (CTP) cards and serial crossbar (SBAR) assembly logic cards
- A minimum configuration of six fiber port module (FPM) cards or universal port module (UPM) cards for both Intrepid Directors, to a maximum configuration of 16 FPM/UPM cards for the Intrepid 6064 and a maximum configuration of 35 UPM cards for the Intrepid 6140.

  Each FPM card provides four 1 Gbps Fibre Channel port connections through LC-Duplex small form factor (SFF) fiber-optic transceivers. Each UPM card provides four 2 Gbps Fibre Channel port connections through SFF fiber-optic transceivers.

  The Intrepid 6140 is only offered with 2 Gbps UPM and CTP cards.

  For both FPM and UPM cards, short wavelength (SX) laser transceivers are available for transferring data over either 50 micron or 62.5 micron multimode fiber cable. Long wavelength (LX) laser transceivers are available for transferring data over 9 micron single mode fiber cable. Fiber optic cables attach to Director port transceivers with LC-Duplex connectors.
- The power module assembly at the rear of the Director also provides a 9-pin, D-type subminiature maintenance port for connection to a local terminal or remote terminal.

Protocol intermix

The McDATA Intrepid Directors support Fibre Channel Protocol (FCP) and FICON protocol intermix at the port level. If protocol intermix is used on the same Director, FCP and FICON ports should be isolated by zoning.

Note: Protocol intermix is not supported by zSeries servers at this time. However, it is expected to be available during the first half of 2003.

Interconnection
With firmware version 4.1.0 (Build 12) and above, the McDATA Intrepid FICON Directors support High-Integrity Fabric (Feature Code 6006 for the Intrepid 6064 or Feature Code 6007 for the Intrepid 6140), which is required for cascaded FICON Directors configuration.

2.1.2 Management capabilities

Fabrics can be managed using different communication methods:

- Enterprise Fabric Connectivity Manager (EFC Manager), IP based client/server configuration management software
- Simple network management protocol (SNMP)
- Serial interface (RS232, dedicated for McDATA and IBM engineers)
- Call home (modem connection for notification purposes)
- Command line interface (CLI)

The most commonly used interface with the McDATA Intrepid Directors are the EFC Server and the Product Manager applications.

The EFC manager is a Java-based graphical user interface (GUI) that enables the user to administer users and products, and monitor products and the interface with the Product Manager applications.

The EFC Manager and Product Manager applications are separate applications; however, the Product Manager is only accessible through the EFC Manager.

The EFC Manager and Product Managers are installed on the EFC Server to provide local access to managed products. These applications can also be installed on remote user workstations to provide access to managed products. A maximum of four concurrent remote users (in addition to the local EFC Server user) can log in to the EFC Manager application. One EFC Server can support up to 48 McDATA FICON Directors.

An example of a Hardware view (default view of a product manager) is shown in Figure 2-1.

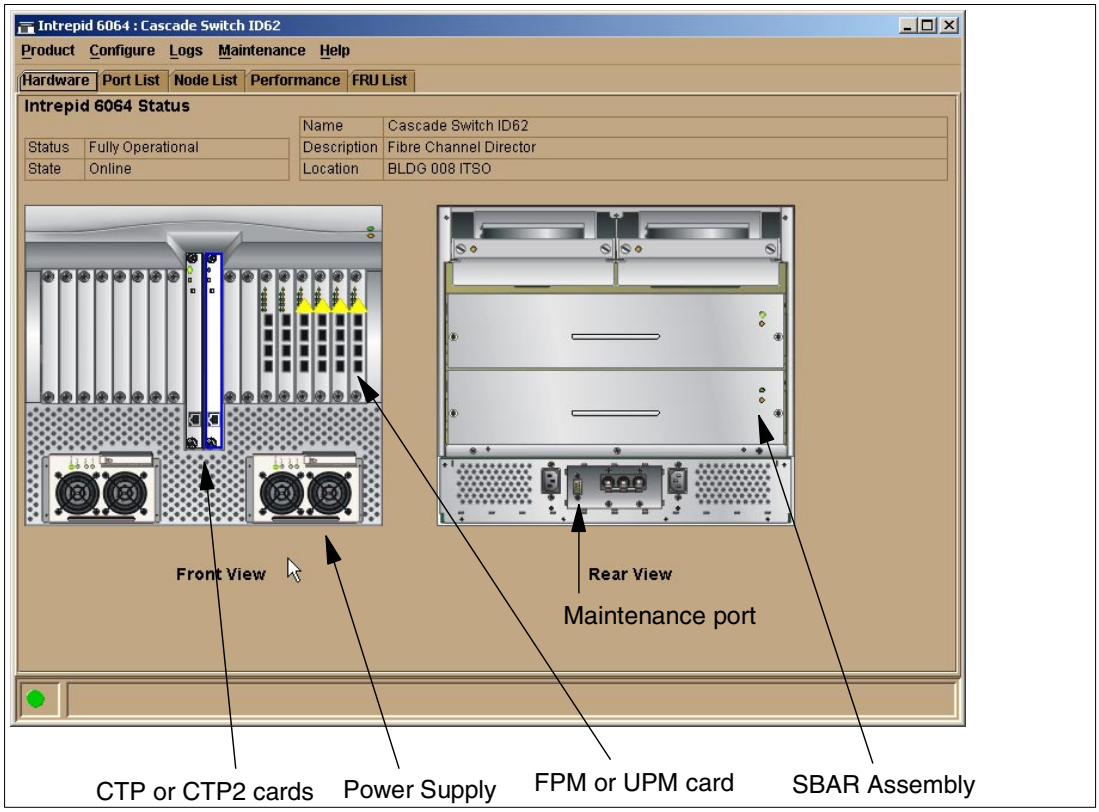


Figure 2-1 Example of EFC Manager Hardware view of an Intrepid 6064 Director

2.1.3 EFC Server hardware requirements

The following list summarizes hardware specifications for the EFC Server notebook platform. Current platforms may ship with more enhanced hardware such as a faster processor, additional random-access memory (RAM), or a higher-capacity hard drive or removable disk drive.

- Notebook PC with color monitor, keypad, keypad-mounted track-ball (mouse)
- Intel processor with 650 Mhz or greater clock speed, running the Microsoft Windows NT 4.0 operating system
- 2 GB or greater internal hard drive
- 128 MB or greater RAM
- CD-ROM drive
- 1.44 MB 3.5-inch floppy disk drive
- 56 k external modem
- Two 10/100 Mbps Ethernet adapters with RJ-45 connectors:
  - Ethernet adapter 1 - Built in the EFC Server motherboard
  - Ethernet adapter 2 - Ethernet adapter card

The EFC Server and external modem are mounted in a slide-out drawer in the Fabricenter cabinet. The EFC Server and managed Directors connect through a 10/100 BaseT Ethernet hub. The 24-port hub is installed at the top of the Fabricenter cabinet. Cabinets can be daisy-chained through the hub.

An EFC Server failure does not affect port connections or functions of an operational Director. The only operating affect of a server failure is loss of remote access, configuration, management, and monitoring functions.

Chapter 4, “Setting up the EFC Server environment” on page 35, and Chapter 5, “Configuring the FICON Director” on page 45 discuss the EFC Manager functions in more detail.

2.1.4 Hardware components

Fiber Port Module (FPM) and Universal Port Module (UPM) cards

The port cards (FPM and UPM) are to provide the physical connectivity between the McDATA Intrepid Director and the external connected devices.

- FPM

  Each FPM card provides four full-duplex generic ports (G_ports) that transmit or receive data at 1 Gbps. Single mode or multimode fiber optic cables attach to pluggable SFF transceivers with LC-Duplex connectors.

- UPM

  Each UPM card provides full-duplex generic ports that transmit or receive data at 1 Gbps or 2 Gbps. UPM cards use non-open fiber control (OFC).

  Each FPM or UPM faceplate contains a number of LEDs, as follows:

  – An amber light (at the top of the card) illuminates if any port or other card circuitry fails, or blinks if FRU beaconing is enabled.

  – One amber LED and one green LED above each port, indicate port status as follows:

    - The green LED illuminates (or blinks if there is active traffic) and the amber LED goes out to indicate normal operation.
    - The amber LED illuminates and the green LED goes out to indicate a port failure.
    - Both LEDs extinguish to indicate a port is operational but not communicating with an N_Port (no cable attached, loss of light, port blocked or link recovery in process).
    - The amber LED flashes and the green LED either remains on, goes out or flashes to indicate a port beaconing or running online diagnostics.

Control Processor (CTP)

The Directors are delivered with two CTP cards. The active card initializes and configures the Director after power on and contains the microprocessor and associated logic that coordinate Director operation. A CTP card provides an initial program load (IPL) button on the faceplate. When the button is pressed and held for three seconds, the Director reloads firmware and resets the CTP card without switching off power or affecting operational fiber-optic links

Each CTP card also provides a 10/100 megabit per second (Mbps) RJ-45 connector on the faceplate that attaches to an Ethernet local area network (LAN) to communicate with the EFC Server or a simple network management protocol (SNMP) management station. Each CTP card must have a separate Ethernet connection to the EFC Server.

Each CTP card provides system services processor (SSP) and embedded port (EP) subsystems. The SSP subsystem runs Director applications and the underlying operating system communicates with Director ports and controls the RS-232 maintenance port and the 10/100 Mbps Ethernet port. The EP subsystem provides class F and exception frame processing, and manages frame transmission to and from the SBAR assembly. In addition, a CTP card provides nonvolatile memory for storing firmware, Director configuration information, persistent operating parameters, and memory dump files.

Note: Director firmware is upgraded concurrently (without disrupting operation).

The backup CTP card takes over operation if the active card fails. Failover from a faulty card to the backup card is transparent to attached devices.

Each card faceplate contains a green LED that illuminates if the card is operational and active, and an amber LED that illuminates if the card fails. Both LEDs are extinguished on an operational backup card. The amber LED blinks if FRU beaconing is enabled.

Power supply

Redundant, load-sharing power supplies step down and rectify input power to provide 48-volt direct current (DC) power to Director FRUs. The power supplies also provide overvoltage and overcurrent protection. Either power supply can be replaced while the Director is powered on and operational.

Each power supply has a separate backplane connection to allow for different AC power sources. The power supplies are input rated at 85 to 264 volts alternating current (VAC). The faceplate of each power supply provides the following status LEDs:

- A green PWR OK LED illuminates if the power supply is operational and receiving AC power
- An amber FAULT LED illuminates if the power supply fails
- An amber TEMP LED illuminates if the power supply shuts down due to an over temperature condition
- An amber I LIM LED illuminates if the power supply is overloaded and operating at the current limit which is 15.6 amperes.

RFI shield

The RFI shield covers and provides RFI protection for all rear-access FRUs, except the power module assembly. The RFI shield is concurrent and can be removed or replaced while the Director is powered on and operating.

Power Module Assembly

The power supply assembly is located at the bottom rear of the Director.

Important: The module is a non-concurrent FRU and the Director must be powered off prior to removal or replacement.

The module provides the following:

- Two single-phase AC power connectors. Each connector's input rated is 85 to 264 VAC.
- A power switch (circuit breaker) that controls AC power distribution to both power supplies. The breaker is set manually or is automatically tripped by internal software if thermal sensors indicate the Director is overheated.
- A 9-pin maintenance port that provides a connection for a local terminal or dial-in connection for a remote terminal. The port is used by maintenance personnel to configure network addresses
- An input filter and AC system harness (internal to the FRU) that provides the wiring to connect AC power connectors to the power switch and power supplies (through the backplane).

Fan Module

Two Fan Modules, each containing three fans, provide cooling for the Director FRUs, as well as redundancy for continued operation if a fan fails.

A Fan Module can be replaced while the Director is powered on and operating. An amber LED illuminates if one or more fans fail or rotate at insufficient angular velocity.

Attention: A failing Fan Module must be replaced within ten minutes after its removal, otherwise, internal software will power off the Director.

SBAR assembly

The Director is delivered with two SBAR assemblies. The active SBAR is responsible for Fibre Channel frame transmission from any Director port to any other Director port. Connections are established without software intervention. The assembly accepts a connection request from a port, determines if a connection can be established, and establishes the connection if the destination port is available. The assembly also stores busy-source connections and error status for each Director port.

The backup SBAR takes over operation if the active assembly fails and provides the ability to maintain connectivity and data frame transmission without interruption. Failover to the backup assembly is transparent to the attached devices.

Each SBAR assembly consists of a card and steel carriage that mounts flush on the backplane. The carriage provides protection for the back of the card, distributes cooling air flow, and assists in aligning the assembly during installation. The rear of the carriage contains a green LED that illuminates if the assembly is operational and active, and an amber LED that illuminates if the assembly fails. Both LEDs are extinguished on an operational backup assembly. The amber LED blinks if FRU beaconing is enabled.

Backplane

The backplane provides 48 VDC power distribution and connections for all logic cards.

Important: The backplane is a non-concurrent FRU. The Director must be powered off prior to FRU removal and replacement.

2.1.5 FICON Director configurations

McDATA FICON Directors can be configured in 4-port increments, and are available in two different models (see Figure 2-2):

- Intrepid 6064, which supports a minimum of 24 ports and a maximum of 64 ports
- Intrepid 6140, which supports a minimum of 64 ports and a maximum of 140 ports

The Intrepid 6040 supports FPM and UPM cards, however, the Intrepid 6140 only supports UPM cards. All port cards (FPM or UPM) are hot-pluggable.

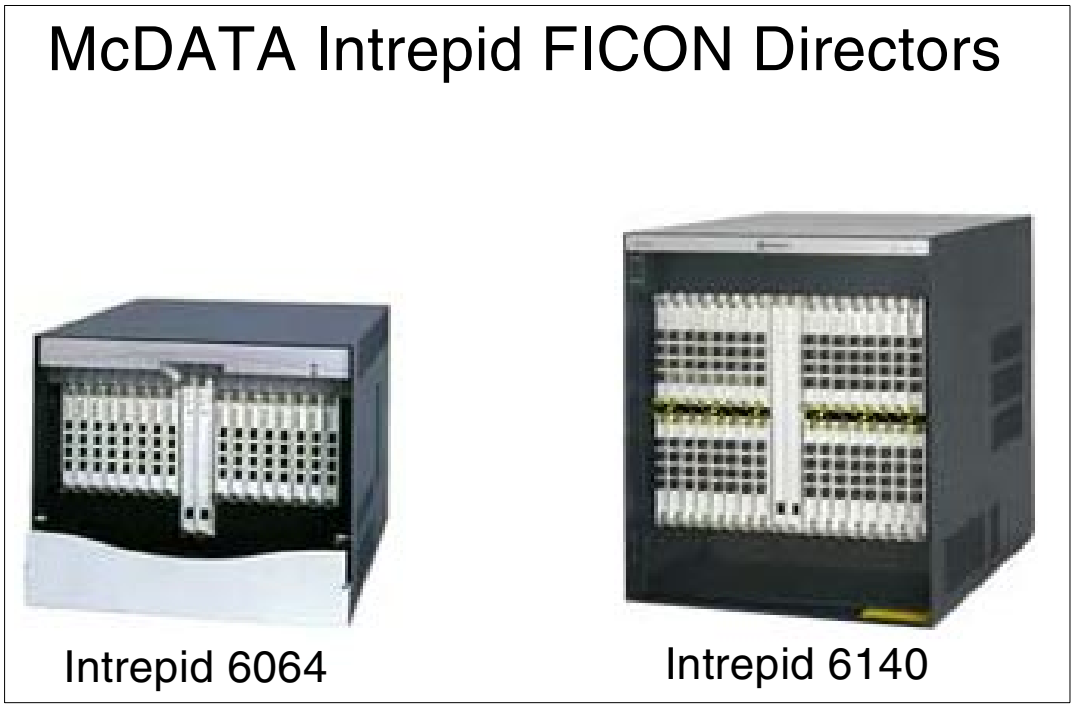


Figure 2-2 McDATA Intrepid FICON Director models

The Directors come standard with all high-availability features in the base unit. You need only to select the number and type of port cards, the rack-mounting brackets (for factory or field installation in an FC-512 cabinet), and the power cord.

The Director's high-availability configuration offers redundancy and maintenance capabilities such as:

- All active components are redundant.
- Active components provide support for automatic failover.
- Redundant power and cooling
- Hot swapping of all FRUs
- Automatic fault detection and isolation
- Non-disruptive firmware updates

Any unused FICON port or entire card can be used as a spare to take over operation for a failed port or card. To continue operation, fiber cables from the failed ports have to be reconnected to the unused operating ports.

2.1.6 FICON SANtegrity feature

If you intend to establish a FICON cascaded Director environment, it is mandatory that the two Directors are put into a High Integrity Fabric. To do this, Feature Code 6006 for the Intrepid 6064 or Feature Code 6007 for the Intrepid 6140 (known as FICON SANtegrity), must be enabled. This feature includes Fabric Binding and Insistent Domain ID functions, as part of *Enterprise Fabric Mode*.

Note: Be aware that the FICON Directors used for a cascaded environment must be from the same vendor, and both must be on the same firmware level.

During channel initialization (if connected to a cascaded environment) the high integrity feature will be checked to ensure Enterprise Fabric Mode is enabled, by using a new command (Query Security Attributes). If this feature is not present or enabled, channel initialization will not continue.

Section 5.2, “Activating the High Integrity feature” on page 48, describes how to establish Fabric Binding.

2.1.7 Control Unit Port (CUP)

The CUP is supported by the McDATA Intrepid FICON Directors, and is known as FICON Management Server (Feature Code 6302 for the Intrepid 6064 or Feature Code 6003 for the Intrepid 6140). The CUP function allows z/OS or OS/390 to manage the Director with the same level of control and security as it is known from an ESCON switch. Host communication includes control functions like blocking/unblocking ports, as well as monitoring and error reporting functions.

Note: The McDATA FICON Director must also be defined in the IOCP as device type 2032 for this function to work.

System Automation (SA) I/O-Ops V2.1 includes support for FICON Native (FC) channels and FICON Directors. APAR OW47972 is required to correct a problem with the FICON Director support.

SA I/O-Ops V1.3 adds support for FICON Native (FC) channels and FICON Directors with APAR OW40040 (PTFs UW69057 for RA30 and UW69058 for RA3U). APAR OW48434 is also recommended.

Before using I/O-Ops within a FICON configuration, check the latest maintenance recommendations in the product’s PSB buckets.

Table 2-1 SA OS/390 I/O-Ops PSP buckets

Upgrade	Subset
HKYS100	HKYS100
JKYS103	JKYS103

For additional z/OS and OS/390 information, refer to the *FICON Native Implementation and Reference Guide*, SG24-6266.

3

Pre-installation planning

This chapter provides information and recommendations for planning the installation of a McDATA Intrepid FICON Directors for attachment to FICON or FICON Express channels on zSeries and 9672 G5/G6 servers.

The following topics are discussed and/or described in this chapter:

- Planning considerations
- Physical port layout
- IP addressing
- Switch numbering
- Fabric binding and Insistent Domain IDs
- Zoning
- Cables and connectors
- zSeries and 9672 G5/G6 FICON channel support

© Copyright IBM Corp. 2003. All rights reserved.

3.1 Planning recommendations

The following items should be considered during the installation planning phase of the McDATA Intrepid FICON Directors:

- Which topology will be implemented?
  - Switched point-to-point topology. For a more detailed explanation of this topology refer to 1.3.1, “Switched point-to-point configuration” on page 6.
  - Cascaded FICON Directors topology. For a more detailed explanation of this topology refer to 1.3.2, “Cascaded FICON Director configuration” on page 8.
  - Mix of both switched point-to-point and cascaded FICON Directors
- How many channels and control unit (CU) ports will be connected to each FICON Director?
  - The number of channels and CU ports to be connected to each Director depends on the number of FICON channels on the server(s) and CU ports on the devices, as well as the individual performance, availability, and growth requirements.
- How should the channels, CU ports, and/or Inter-Switch Links (ISLs) be distributed among the FPM/UPM cards in the Director(s)?
  - Each FICON Director layout should satisfy all availability, performance, and growth requirements. Refer to 3.3, “IP addressing and connectivity” on page 23.
- Should the Switch IDs in the IOCP definitions and switch addresses in the FICON Directors match?
  - We recommend using the same IDs/addresses in both places to avoid any potential errors that could be caused by having two different values.
- Should zoning be used to separate specific channels and CU ports from other connected channels and CU ports?
  - Zoning is recommended if there is a requirement to prevent random access to confidential data (see 3.6, “Zoning” on page 30).

  Important: Zoning is highly recommended in a mixed environment with FICON and FCP devices connected to the same Director. Protocol intermix is expected to be available for zSeries servers during the first half of 2003.

- Should the FICON Director(s) and the Enterprise Fabric Connectivity (EFC) Sever be connected to a separate LAN or to the corporate network?
  - The Director(s) and EFC Manage workstation should always be interconnected on a separate LAN, known as the service LAN to isolate Director management traffic from other IP traffic. However, if remote access is required to operate and maintain the FICON Director(s), then we recommend that the EFC Sever be connected to the corporate network via a second LAN adapter. Refer to 3.3, “IP addressing and connectivity” on page 23.
- What are my fiber optic cabling requirements?
  - Can the existing fiber optic cables, patch panels, and trunk cables be reused?
  - Are Mode Conditioning Patch (MCP) cables and/or conversion kits required?
  - Is there a link distance constraint?

  Refer to 3.7, “Cables and connectors” on page 31, and 3.8, “FICON channel support for zSeries and 9672 G5/G6 servers” on page 32 for more information.

3.2 Physical port layout

Before installing the FICON Director, consider where to connect your FICON channels from the server and the control unit ports, as well as the ISLs (if applicable), based on your requirements.

- Distribute the channels among different FPM/UPM cards.

  If two channels are defined to access the same CU, plug both fiber optic cables into different FPM/UPM cards in the Director.

- Distribute the CU ports among different FPM/UPM cards.

  If two paths are defined to attach the CU to the server via a Director, connect both fiber optic cables to ports on different FPM/UPM cards.

- Distribute the ISLs across different FPM/UPM cards.

  If two or more ISLs are to be attached between the Directors, then connect the fiber optic cables to ports on different FPM/UPM cards.

Following these simple rules will assure that there is always one path available between the server and the CU in case of a defective FPM/UPM card in the Director.

Refer to Appendix B., “Port location and mapping” on page 79 for physical port locations, and port numbering and port addresses on the FPM/UPM cards.

In Appendix C, “FICON Director configuration worksheet” on page 85, you will find a worksheet to help with documenting the physical layout of your FICON Director(s).

3.3 IP addressing and connectivity

For controlling and maintaining the McDATA FICON Director, both CTP cards in each Director have connectivity to the EFC Sever via an Ethernet LAN, known as the service LAN. An Ethernet hub is installed in each cabinet, which is used to connect all the CTP cards and the EFC Manager workstation.

Although two CTP cards are installed in each Director, only one IP address is required for both CTP cards. The Ethernet port on the *backup* CTP card is deactivated, and only the port on the currently *active* CTP card is activated. In case of a failure of the active CTP card, the Ethernet port of the backup CTP is automatically activated.

The default IP address for the CTP card is 10.1.1.10, and for the EFC Manager it is 10.1.1.1 with a default subnet mask of 255.0.0.0. The default gateway address is 0.0.0.0.

If the Director and the EFC Sever are to be connected to a corporate network instead of the service LAN, then their IP addresses and subnetwork mask have to conform to the IP addressing standard used in the corporate network.

A minimum of two IP addresses are required; one address for the CTP cards, and one address for the EFC Sever.

If it is required to alter the IP address and/or subnetwork mask of a Director, for example, when multiple Directors are on the same service LAN, refer to Appendix , “Altering an IP address in a CTP card” on page 74.

The recommended network configuration for the Director, the EFC Sever, and client workstation is shown in Figure 3-1.

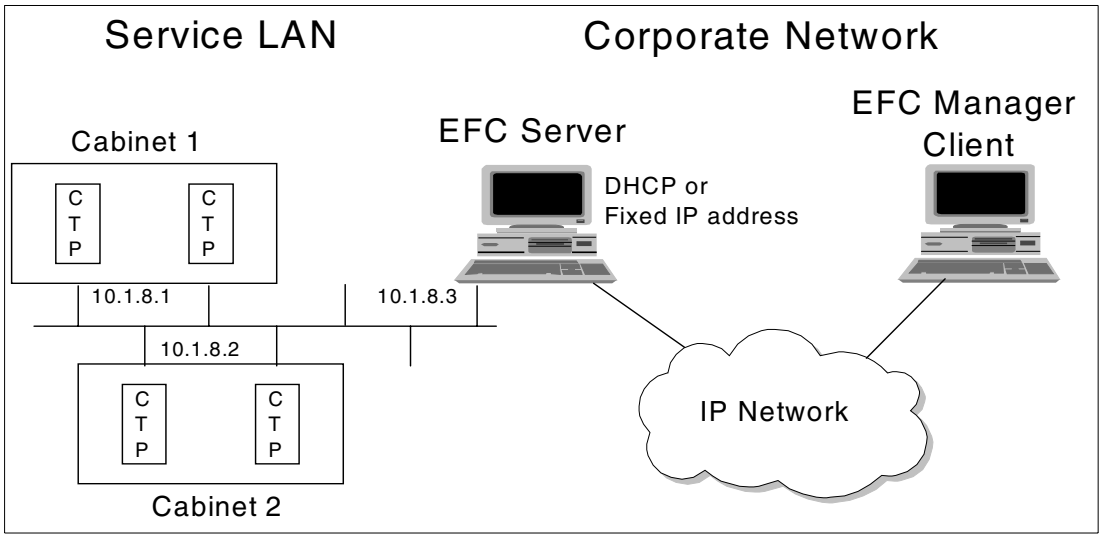


Figure 3-1 Recommended network connections

In this configuration, the EFC Sever has two Ethernet adapters installed; one to connect the FICON Director and EFC Sever via the service LAN, and the second to provide connectivity for the client workstation via the corporate network.

Figure 3-2 shows EFC Manager display of the actual IP address of our FICON Directors.

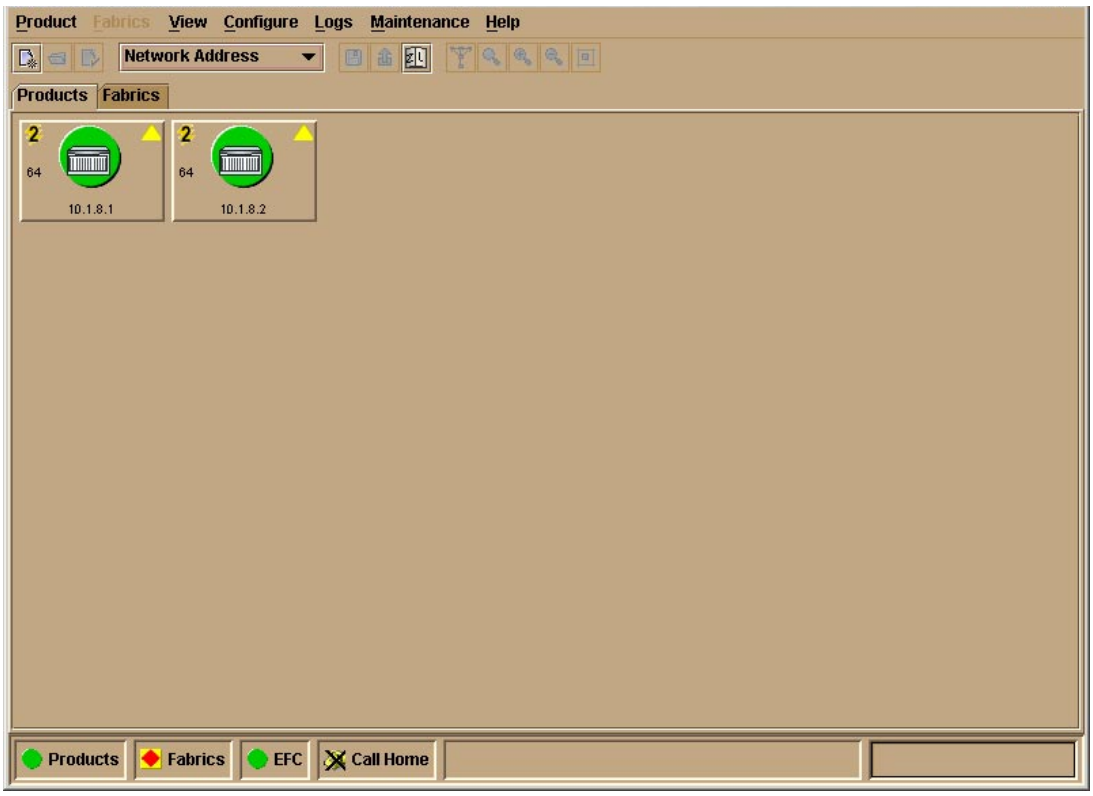


Figure 3-2 Display IP address of a Director

Chapter 4, “Setting up the EFC Server environment” on page 35 describes the necessary steps for setting up the EFC Manager environment.

3.4 Switch numbering

Each FICON Director in a fabric must have a unique switch address (Domain ID) and a unique Switch ID. This Switch ID is used in IOCDS to define the link between the FICON channel and CU. The Switch ID can be any value between x'00" to x'FF', while the switch address range may be restricted by the FICON Director firmware.

The valid switch address range for a McDATA Director is between x'61' to x'7F'. When defining the switch number and link addresses in the IOCP definitions, ensure that you use values within this range.

The switch address is built for the Director by adding an offset of x'60' to the switch Domain ID, which is entered as a decimal value when the Director is configured.

While 0 is an invalid Domain ID, the switch ID number can range between 1 to 31. So, a total of 31 Domain IDs is available.

This means, defining a Domain ID of 1 in the Director builds a switch address of x'61' and a Domain ID of 31 results in a switch address of x'7F'.

It is important to point out that some definition terms used in the IOCP and HCD are carried over from the ESCON environment. An example of the terms used, and how they relate to the FICON environment are shown in Figure 3-3.

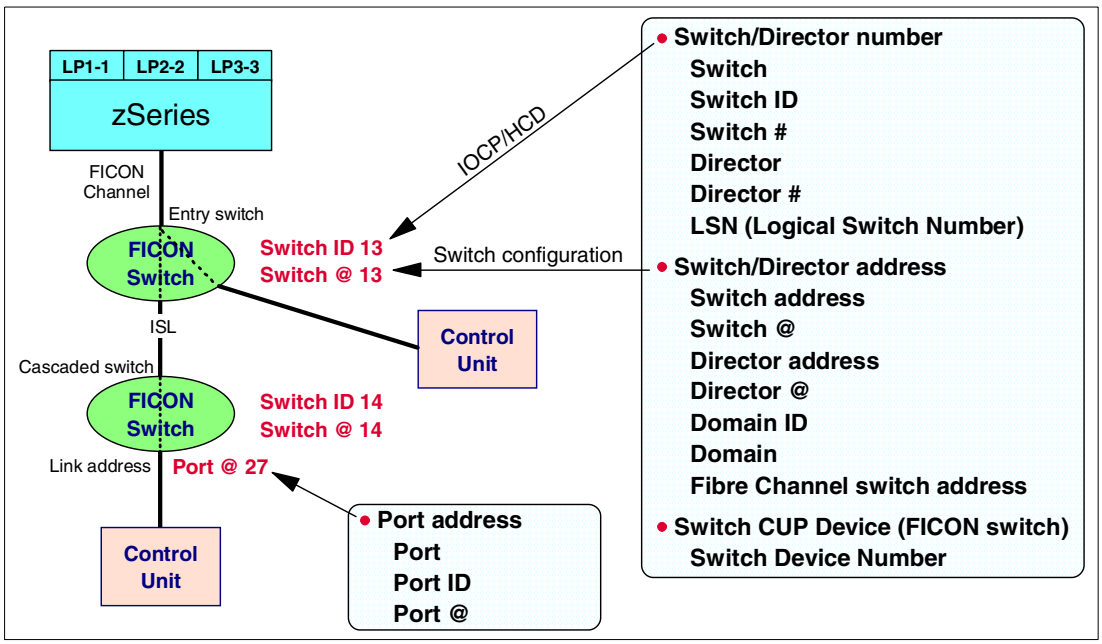


Figure 3-3 Term usage with FICON Directors

- The Switch ID has to be assigned by the user, and must be unique within the scope of the definitions (IOCP and HCD).
- The switch address is assigned by the manufacturer, and may be customized to a different value and must be unique within the fabric.

We recommend that the Switch ID be set to the same value as the switch address of the FICON Director, which is defined to the FICON Director at installation time. This will simplifies the configuration and reduce confusion by having a common designation across all definitions.

Note: These rules should be followed not only for a cascaded FICON Director configuration, but also for a switched-point-to-point configuration. If any single switch is to be merged into a fabric in the future, there will be no need to change the switch address (Domain ID) setting, which is a disruptive action.

While the Switch ID in the CHPID statement is a logical switch number and defines the entry point to the fabric, the link address in the CNTLUNIT statement points to the exit port of the fabric.

In a switched point-to-point configuration shown in Figure 3-4, the logical switch number is used in IOCP to define the entry point to the fabric. This is done using the SWITCH keyword. For the exit port, a 1-byte destination link address value must be defined with the LINK keyword. This value is the FICON Director port address of the physical port that the CU is attached to.

Important: It is possible to define a 2-byte link address (switch address and port address). However, the FICON Director must have the Fabric Binding and Insistent Domain ID feature installed and configured. Refer to 3.5, “Binding and Insistent Domain ID” on page 28 for more details.

Also, once a 2-byte link address is defined to a channel path, all link addresses defined to be accessed from that same channel path must be 2-byte link addresses.

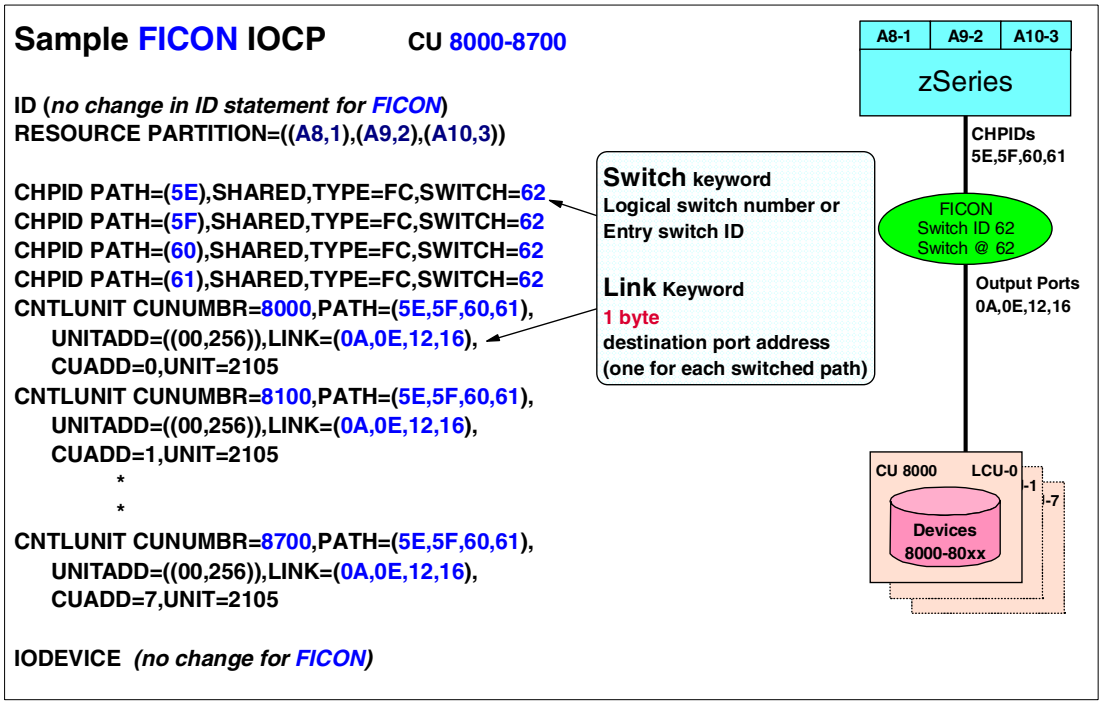


Figure 3-4 Sample IOCP coding for switched point-to-point configuration

For a cascaded switch configuration refer to Figure 3-5 for the relation between Switch IDs and link address definitions in the IOCDS, and the switch address settings in the FICON Director. For the exit port, you must define a 2-byte link address value (destination switch address and port address) in the LINK keyword.

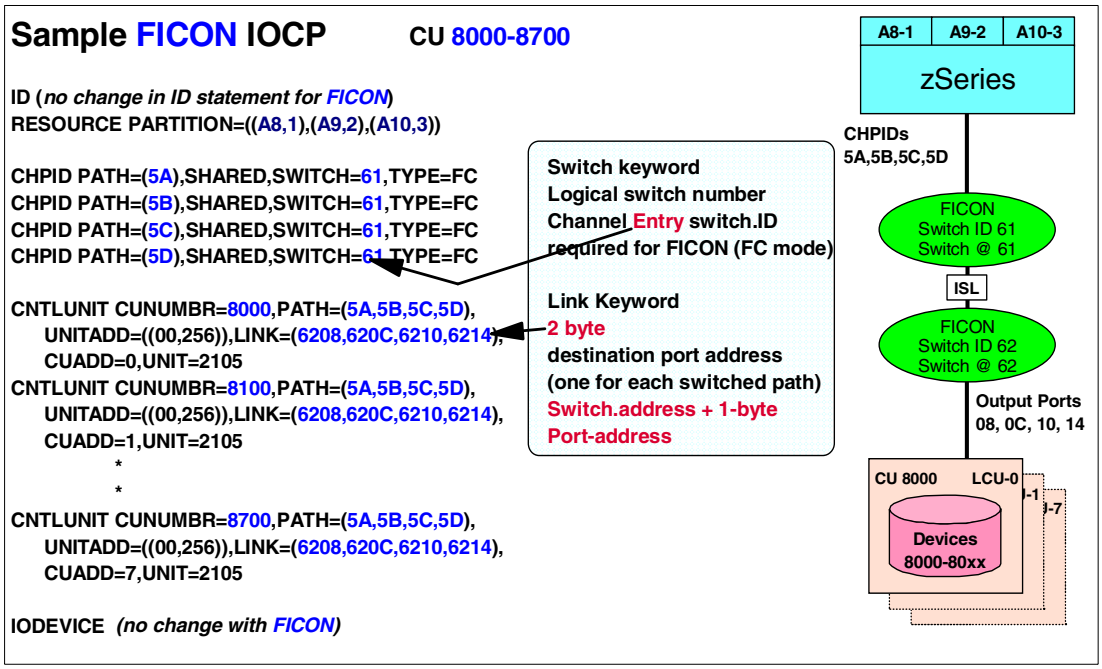


Figure 3-5 Sample IOCP coding for cascaded FICON Directors configuration

During installation of the FICON Director, a valid switch address has to be assigned. The Director has a defined switch address, which can be altered to match the customer requirements.

Figure 3-6 shows the system configuration panel where the switch address (Director Domain ID) can be altered. This value has to be entered as a decimal value, and is then calculated to hexadecimal value by the firmware.

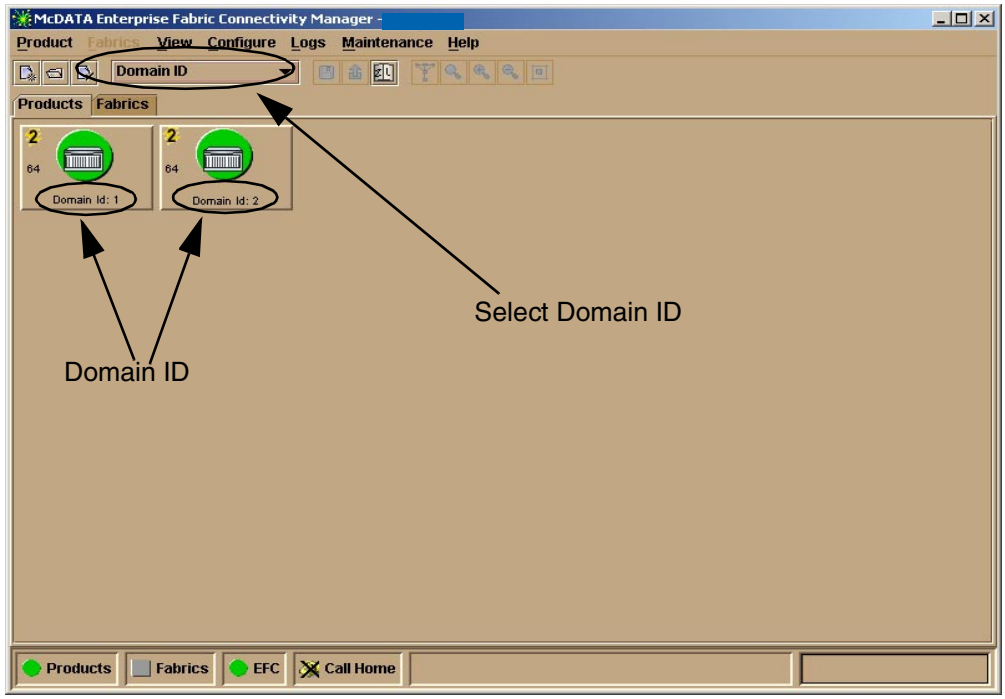


Figure 3-6 Domain ID screen

Inter-Switch Links (ISLs) defined to HCD

If HCD is used to build the IOCDS, we suggest the ports used for ISLs be marked as “occupied” in HCD. This prevents accidental attempts to define these ports to channels or CUs.

If you are not familiar with HCD, refer to *Input/Output Configuration Program Users Guide,* SB10-7029 at:

http://www.ibm.com/servers/resourcelink

An example for this new function in HCD is shown in Figure 3-7.

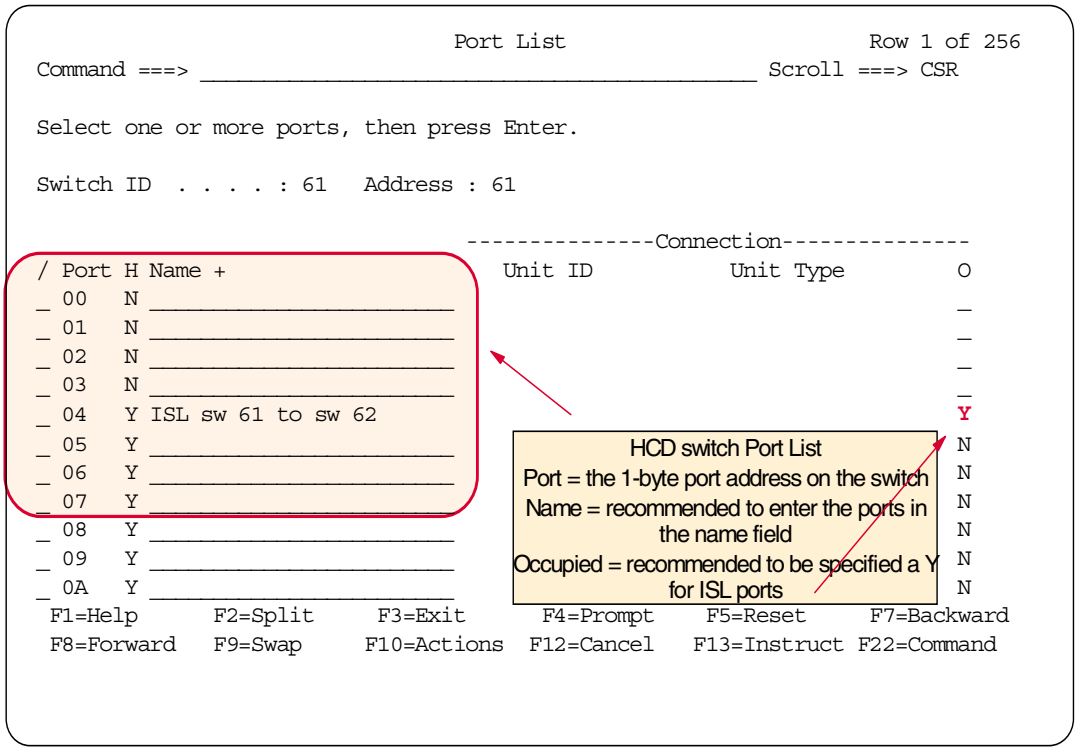

Port List
Row 1 of 256
Command ===>
Scroll ===> CSR
Select one or more ports, then press Enter.
Switch ID . . . . : 61 Address : 61
Connection
/ Port H Name +
Unit ID
Unit Type
O
_ 00 N
_ 01 N
_ 02 N
_ 03 N
_ 04 Y ISL sw 61 to sw 62
_ 05 Y
_ 06 Y
_ 07 Y
_ 08 Y
_ 09 Y
_ 0A Y
Y
N
HCD switch Port List
Port = the 1-byte port address on the switch
Name = recommended to enter the ports in the name field
Occupied = recommended to be specified a Y for ISL ports
F1=Help F2=Split F3=Exit F4=Prompt F5=Reset F7=Backward
F8=Forward F9=Swap F10=Actions F12=Cancel F13=Instruct F22=Command

Figure 3-7 Mark ISL ports as “occupied” in HCD

3.5 Binding and Insistent Domain ID

Insistent Domain IDs prohibit the use of dynamic Domain IDs to ensure predictable Domain IDs are enforced within the fabric. For example, if a switch has this feature enabled, and a new switch is connected to it (via an ISL) without the preferred Domain ID, then the new switch is segmented into a separate fabric and user data will not flow.

Binding is a method used in the switch to prevent devices and/or other switches from attaching to the switch, based on WWNs that are defined to a *membership list*. The McDATA FICON Director supports three levels of binding:

Port binding

This limits the N_Port that can be attached to an F_Port on the FICON Director by WWN.

Port binding requires a *Bound WWN*, which is the device’s N_Port WWN (WWPN) that connects to a particular F_Port on the FICON Director.

Attaching an unauthorized N_Port to the FICON Director puts the F_Port into an “Invalid Attachment” state, and renders the port unusable until the assigned N_Port is attached.

Since an N_Port is mapped directly to an F_Port within the FICON Director, there are some flexibility limitations with port binding. For example, port swapping within a FICON Director requires modifying the Bound WWN. See 5.5.3, “Configuring a port” on page 61 for an example.

Switch binding

This limits the nodes that can be attached to a FICON Director by WWN.

Switch binding requires a switch membership list that contains all nodes’ WWNs (WWNNs), of switches or devices that can attach to the FICON Director.

Attaching unauthorized nodes puts the FICON Director’s port (F_Port) into an “Invalid Attachment” port state, because their WWNNs are not in the switch membership list.

This type of binding allows for more flexibility since an N_Port is not bound to an F_Port, and so port swapping can be done without changes to the switch membership list. However, moving a device from one FICON Director to another requires changes to the switch membership lists.

Fabric binding

FICON Directors that are allowed to connect to the fabric must be added to the fabric membership list of each FICON Director within the fabric. The fabric membership list is composed of the WWNN and Domain ID of each FICON Director permitted to communicate within the fabric.

Exchanging fabric membership data is a Switch Fabric Internal Link Service (SW_ILS). The fabric membership list is exchanged between connected switches in the fabric before path selection is started.

If an unauthorized FICON Director port (E_Port) is attached to another Director, then the port between the two switches will be placed in an “Invalid Attachment” state.

Fabric binding is a software-enforced security feature that permits an administrator to control the switch composition of a fabric by explicitly defining which switches are capable of forming a fabric. Thus, an operator is able to prevent non-authorized switches access to a fabric. A non-authorized switch attempting to gain entry to a fabric becomes isolated by embedded software.

Fabric binding also validates that the formation about any inter-switch link (ISL) between previously unconnected switches is not restricted. If the establishment of the ISL is not authorized the link is isolated and the state of the associated E_Port is updated to reflect the “Invalid Attachment.”

In addition to ISL verification, fabric binding provides in-band propagation of fabric membership data updates to all switches within a fabric, thus ensuring a consistent and unified behavior across all potential fabric access points.

When an ISL becomes available the switch on either end of the fiber may verify that fabric binding and insistent Domain ID are supported and enabled on the adjacent switch. If both sides of the ISL support fabric binding, each switch verifies that the newly-connected neighbor switch and all switches in the adjacent fabric (of which the neighbor switch is a member) are authorized to form a fabric, or expand the current fabric. If authorization is not granted, the switch on which the authorization check failed isolates the link and sets the corresponding port state to “Invalid Attachment.”

Figure 3-8 shows a cascaded FICON Director environment with high integrity. The FICON Director prevents FC frames (user-data streams) from being delivered to the wrong destination if cables are incorrectly connected.

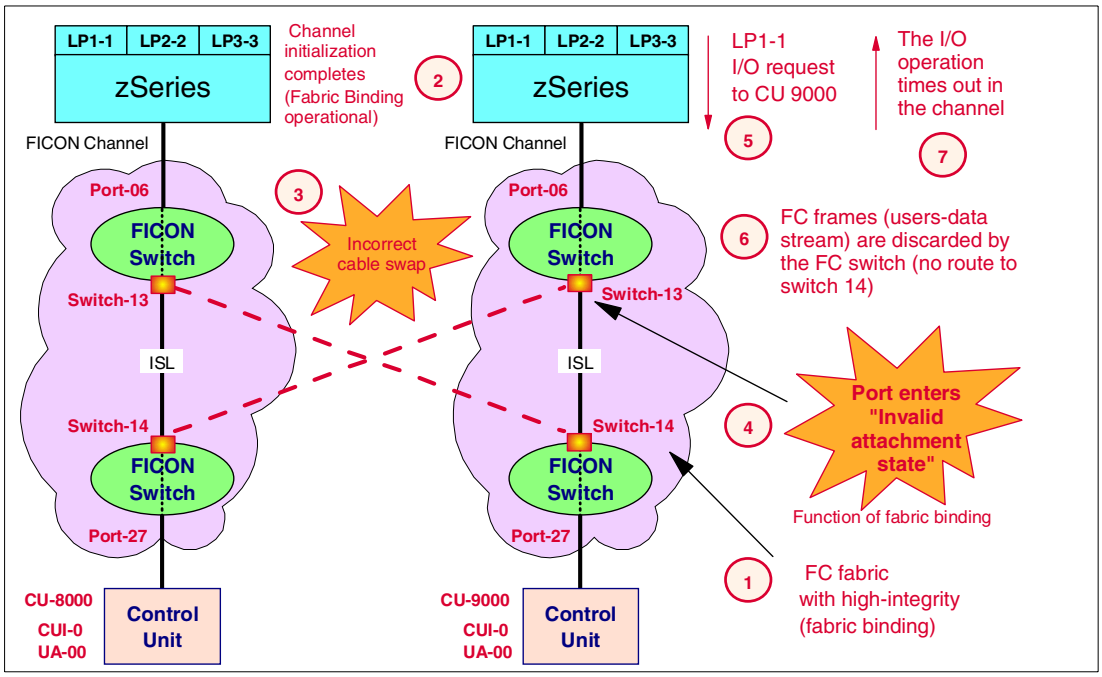


Figure 3-8 Cascaded FICON Directors with Fabric Binding and Insistent Domain IDs

Restriction: Fabric binding is required for FICON support of cascaded Director, and switched point-to-point configuration when a 2-byte link address is used.

3.6 Zoning

Zoning is a method to enable or disable communication between different ports and between attached devices (based on WWN). You can put a group of ports or WWNs into the same zone to enable communication only between those ports or WWNs. There are good reasons to zone, for example:

- To prevent non-FICON-capable devices from seeing FICON-capable devices
- To limit the access to devices with confidential data to specific servers
- To control the amount of paths between servers and devices
- In an intermixed environment, restrict FCP traffic from accessing FICON-capable devices

Several zones can be included in one zone set. An active zone set is valid for all switches belonging to the same fabric.

Only one zone set can be active in a fabric at a time, although more than one zone set can be defined in a switch.

For a better understanding of zoning, refer to the configuration example in Figure 3-9.

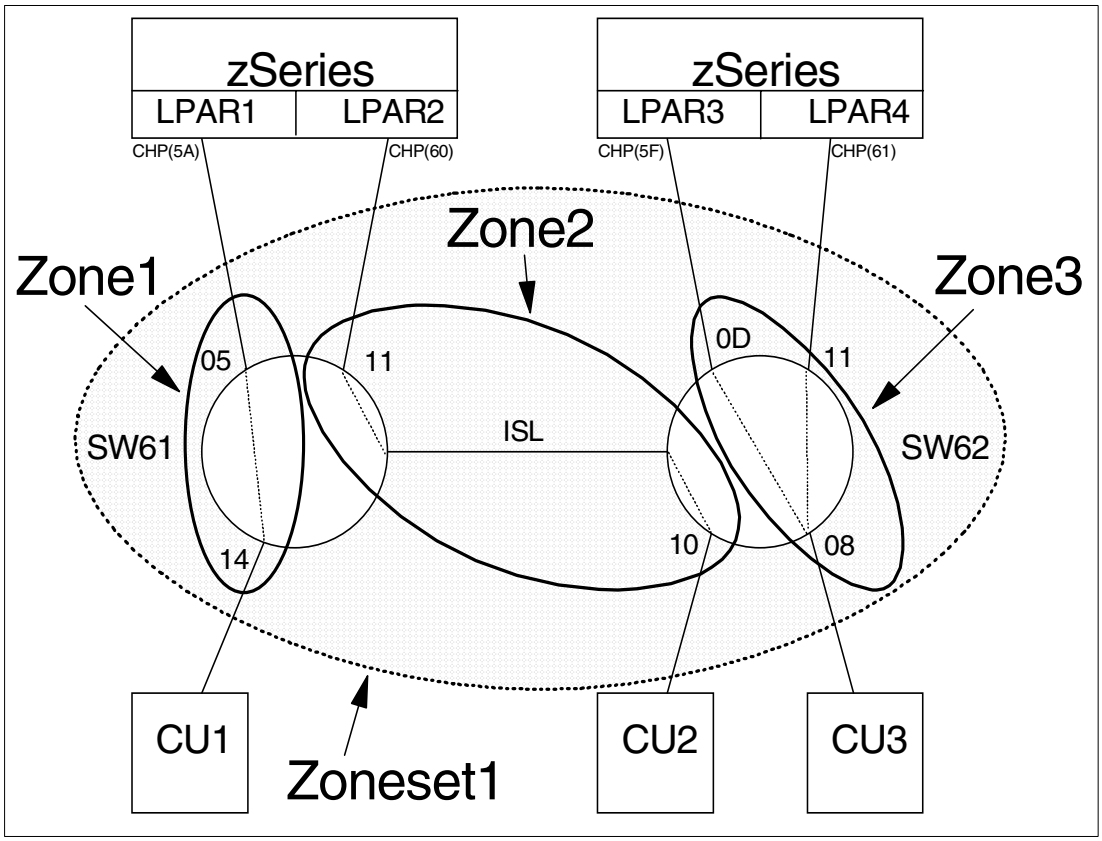


Figure 3-9 Configuration example of zoning

In this example, we have several LPARs with paths to different CUs via two FICON Directors. Each LPAR must get access only to a specific CU, and no access to CUs belonging to other partitions.

To prevent intended access by others, we have grouped the ports belonging to the path between an LPAR and CU into a zone. There are three zones defined as follows:

Zone1 Zone1 has all ports for the path between LPAR1 and CU1, which are Ports 05 and 14 in SW61.

Zone2 Zone2 has all ports for the path between LPAR2 and CU2, which are port 11 in SW61 and port 10 in SW62.

Zone3 Zone3 has all ports for the path between LPAR3 and LPAR4 and CU3 which are port 0D, 11 and 08 in SW62

All three zones are added into Zoneset1.

The link between both switches (ISL) is transparent in the path between LPAR2 and CU2.

3.7 Cables and connectors

Considerations for fiber optic cables and connectors depend on the environment. If there are existing fiber optic cables in the environment, consider about reusing these cables rather than installing new.

The required distance between the FICON channel and the FICON CU has to be considered. Refer to Table 3-3 on page 33 for zSeries and 9276 G5/G6 FICON Channel distance specifications.

Conversion kits may be required if the connectors are of differing types (LC Duplex, SC Duplex, or ESCON Duplex).

When connecting a single mode port of the Director to an existing multimode cable, mode conditioning patch (MCP) cables are required at both ends of the existing multimode fiber optic cable. Verify the MCP cable type (connector, receptacle, and fiber (50 or 62.5 micron)), needed.

Note: With a FICON channel, MCP cables can *only* be used with a link data rate of 1 Gbps (100 MBps). Hence, a link data rate of 2 Gbps is not supported with MCP cables.

3.8 FICON channel support for zSeries and 9672 G5/G6 servers

There are two types of FICON features available: FICON and FICON Express. Both types support a long wavelength (LX) laser version and a short wavelength (SX) laser version for the transceiver.

The z900 is the only server that supports both types of FICON features. However, for new z900 configurations only the FICON Express features is orderable. The z800 family only supports the FICON Express features, whereas the 9672 G5/G6 servers only support the FICON features.

FICON and FICON Express features

Table 3-1 lists the FICON and FICON Express feature codes with the appropriate laser type (short wavelength (SX) or long wavelength (LX)), number of ports per card, and the server type that supports them.

Table 3-1 FICON and FICON Express feature codes

Feature Code	Ports per adapter	9672 G5/G6	z900[a]	z800[b]
FC 2314 (FICON LX)	one	X		
FC 2316 (FICON SX)	one	X		
FC 2315 (FICON LX)[c]	two		X	
FC 2318 (FICON SX)[c]	two		X	
FC 2319 (FICON Express LX)	two		X	X
FC 2320 (FICON Express SX)	two		X	X

a. Can intermix FICON and FICON Express cards at driver level 3C or later.
b. Only supports FICON Express cards.
c. Can no longer be ordered.

Table 3-2 maps the supported FICON topologies to their corresponding FICON and FICON Express feature codes.

Table 3-2 FICON topologies with supported FICON and FICON Express feature codes

FICON topology	FC 2314	FC 2316	FC 2315	FC 2318	FC 2319[a]	FC 2320[a]
Switched point-to-point	Yes	Yes	Yes	Yes	Yes	Yes

FICON topology	FC 2314	FC 2316	FC 2315	FC 2318	FC 2319[a]	FC 2320[a]
Cascaded FICON Directors	No	No	Yes[b]	Yes[b]	Yes[c]	Yes[c]

a. Auto-negotiate (2 Gbps) support
b. LIC CC needed to be enabled
c. DRV3G with MCL(J11206) or later must be applied

Check with your local service representative to ensure your zSeries or 9672 G5/G6 server has the required code levels.

3.8.1 FICON channel distances

The distance supported by the zSeries FICON features is dependent upon the transceiver (LX or SX), the fiber being used (9 micron single mode, or 50 micron or 62.5 micron multimode), and the speed at which the feature is operating. A FICON Express feature supports a link data rate of 1 Gbps or 2 Gbps. A FICON feature supports a link data rate of 1 Gbps. Table 3-3 shows the distance impacts and the link budget impacts of high data rates.

In Table 3-3, a link is a physical connection over a transmission medium (fiber) used between an optical transmitter and an optical receiver. The Maximum Allowable Link Loss, or link budget, is the maximum amount of link attenuation (loss of light), expressed in decibels (dB), that can occur without causing a possible failure condition (bit errors). Note that as the link data rate increases, the unrepeated distance and link loss budget decreases when using multimode fiber.

These numbers reflect the Fibre Channel Physical Interface specification. The link budget is derived from combining the channel insertion loss budget with the unallocated link margin budget. The link budget numbers have been rounded to the nearest tenth of a dB.

Table 3-3 FICON channel distance specifications

		1 Gbps link		2 Gbps link	
Fiber type	**Light source (nanometers)**	**Unrepeated distance**	**Link budget**	**Unrepeated distance**	**Link budget**
9 micron single mode	LX laser (1300 nm)	10 km[a] (6.2 miles)	7.8 dB	10 km[b] (6.2 miles)	7.8 dB
50 micron[c] multimode	LX laser (1300 nm)	550 meters (1804 feet)	5 dB	Not supported	N/A
62.5 micron[c] multimode	LX laser (1300 nm)	550 meters (1804 feet)	5 dB	Not supported	N/A
50 micron multimode	SX laser (850 nm)	500 meters (1640 feet)	3.8 dB	300 meters (984 feet)	2.8 dB
62.5 micron multimode	SX laser (850 nm)	250 meters (820 feet)	2.8 dB	120 meters (394 feet)	2.2 dB

a. An RPQ is available to extend the maximum unrepeated distance up to 20 km
b. An RPQ is available to extend the maximum unrepeated distance up to 12 km
c. Mode conditioning patch (MCP) cables are required

For more information refer to *Fiber Optic Link Planning,* GA23-0367.

For all FICON features using repeaters, the end-to-end distance between the FICON channel and the FICON Director port can be up to 100 km. The same end-to-end distance is also available between the FICON Director port and the control unit port. However, the overall end-to-end distance between the FICON channel and control unit should not exceed 100 km.

3.8.2 FICON channel to control unit characteristics

The control unit vendor must provide all the control unit addressing and connectivity characteristics, as these affect how the control unit can be configured in a FICON environment. The control unit vendor should also provide connectivity recommendations to allow the full exploitation of the control unit capability in a FICON environment.

The following items are dependent on the control unit characteristics:

- Number of installed FICON adapters at the control unit
- Number of logical paths supported by the control unit at each FICON adapter
- Number of logical paths supported by the control unit, when there is only one control unit function within the physical control unit
- Number of logical paths supported by each logical control unit within a physical control unit
- Number of logical control units supported and the LCU address for each LCU
- Number of concurrent I/O transfers per physical control unit
- Number of concurrent I/O transfers per logical control unit
- Number of devices and device unit addresses (UAs) supported per logical control unit

  Some devices may be supported by more than one unit address (UA), each device unit address being supported by a different device number (this is the case for the IBM ESS control unit that supports Base and Alias device addresses). This function is known as Parallel Access Volumes (PAV).
- For each LCU, the base device unit address (UA) and address range per LCU

4

Setting up the EFC Server environment

This chapter describes how to set up the Enterprise Fabric Connectivity (EFC) Server environment.

The following topics are covered:

- Installing the EFC Server
- Checking and altering the FICON Director IP address
- Checking the version of EFC Manager application
- Connecting the FICON Directors and EFC Manager
- Defining the FICON Directors to the EFC Manager
- Checking the firmware version of FICON Director
- Examples of EFC Manager use

© Copyright IBM Corp. 2003. All rights reserved.

4.1 Installation and setup

The first steps to install the McDATA Intrepid FICON Director are described in the installation instructions shipped with the machine. The instructions guide you through the following steps:

1. Unpacking the FICON Director
2. Connecting the FICON Director to power
3. Unpacking and installing the EFC Server

Once these steps are completed, the following steps can be used to help you through the setup process of the Enterprise Fabric Connectivity Manager environment.

Step 1. Checking and altering the IP address

Before connecting the FICON Director and the EFC Manger console to the service LAN, check the defined IP addresses.

If multiple Directors are connected to the same service LAN, check to ensure the IP addresses match your requirements and each CTP card has a unique IP address.

Use a HyperTerminal session a described in “Setting up a HyperTerminal session” on page 72 to get the current IP address of the Director. The default IP address of the Director is 10.1.1.10 and 255.255.0.0 is the default subnetwork mask.

If it is necessary to alter an IP address and subnetwork mask, follow the procedure in “Altering an IP address in a CTP card” on page 74.

Important: Changing the CTP card’s IP address may also require changing the EFC Server IP address to allow connectivity between them.

Step 2. Logging into the EFC Server

On the EFC Server, double click the **McDATA EFC Manager** icon and the EFC Manager login will be displayed. Type in the user ID (`Administrator`) and password (`password`), then press Enter. Note that the user ID and password are case sensitive.

Step 3. Checking the EFC Server version

Once logged into the EFC Manager, click the **Help** tab, then the **About** tab. The current version of the EFC Server application will appear (see Figure 4-1).

Figure 4-1 EFC Server version display

If a newer version is available, it should be installed at this time. See “Installing EFC Manager server software” on page 75 for the proper procedure.

Step 4. Connecting the FICON Director and EFC Server

Connect the CTP, and the EFC Server to the Ethernet hub (known as the service LAN), using UTP cables with RJ-45 connectors.

If remote access to the EFC Server is also required, then we suggest using the configuration depicted in Figure 3-1 on page 24.

Step 5. Defining EFC Manager-to-FICON Director communication

The Director has to be defined in EFC Server to initiate communication between the server and Director. Each Director, which should be managed by the server, has to be defined. The EFC Server supports up to 48 Directors.

Click **Product - New** to define a new Director to the EFC Server. In the New Product panel (shown in Figure 4-2) type in the IP address of the Director, then select the product type. Click **OK** to finish.

Repeat above steps for each Director you want to define on this EFC Server.

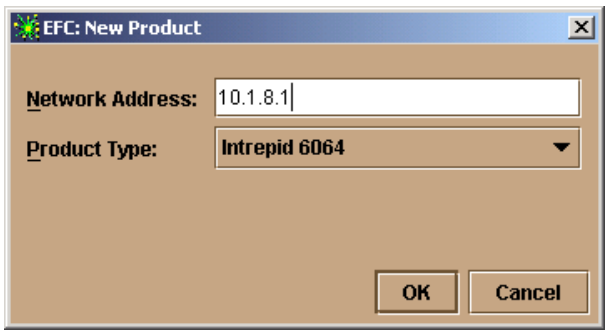


Figure 4-2 Defining new Director

A new icon appears in the EFC Manager for each Director defined via the New Product panel. In the example in Figure 4-3 two Directors with IP address 10.1.8.1 and 10.1.8.2 are defined to the EFC Manager.

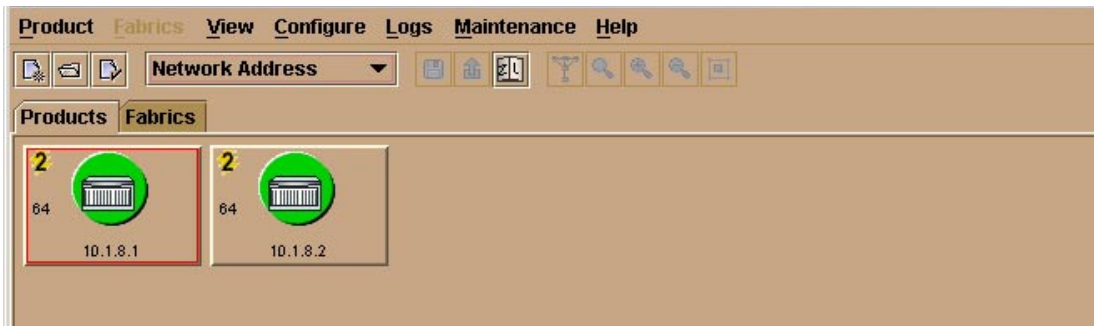


Figure 4-3 Directors added to EFC Manager

If connecting a Director to the EFC Manager was unsuccessful, recheck the current IP address of the Director by selecting the Network Address option. Also, check the physical Ethernet connection of the Director and the EFC Server.

Adding Directors to the EFC Manager only means the Directors are managed by this EFC Manager. Configuring the Directors and a fabric is discussed in Chapter 5, “Configuring the FICON Director” on page 45.

Step 6. Verifying the Director firmware version

Double-click the **Director** icon for the Director you just added in the EFC Manager window. A new window opens displaying the hardware status of the Director.

Click **Product - Properties...** and notice the firmware level of the Director. This is the currently installed and activated firmware in the Director.

Click **Maintenance - Firmware Library..**. to display firmware versions available in the Director. Notice the firmware version from the Firmware library panel shown in Figure 4-4.

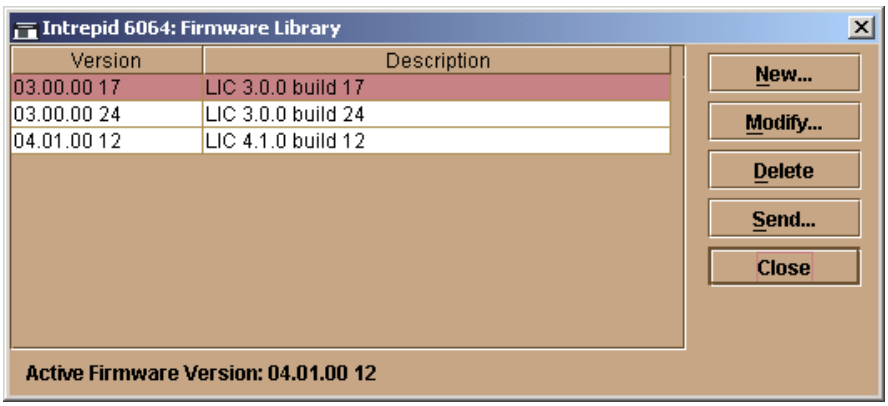


Figure 4-4 Director firmware version

If a newer version of Director firmware is available, it should be installed at this time. See “Upgrading Director firmware” on page 76 for the procedure.

Ready to configure

At this time, the basic installation of the FICON Director and the EFC Server are finished. If you want to access the EFC Server via a separate workstation, then the EFC Manager client has to be installed with the same version level as the EFC Server version level (see “Installing EFC Management client software” on page 76).

You are now ready to configure your FICON Directors and fabrics, however, we suggest that you get familiar with the EFC Manager application, and try some basic functions described in the next section.

4.2 Usage options

Double-click the **EFC Manager** icon and enter the user ID and password in the Logon window to start the session. The Products view opens, as shown in Figure 4-3.

Two view options are available at the top left side of the EFC Manager window:

- Products (default)
- Fabrics

4.2.1 Products

The Products view shows the hardware products managed by the EFC Manager, such as a Director.

For a further breakdown, double-click a **Director** icon. You will find current configuration information of that Director by selecting the tabs at the top of the display:

- Hardware (default)
- Port List
- Node List
- Performance
- FRU List

Figure 4-5 shows a sample display when the Hardware tab is selected.

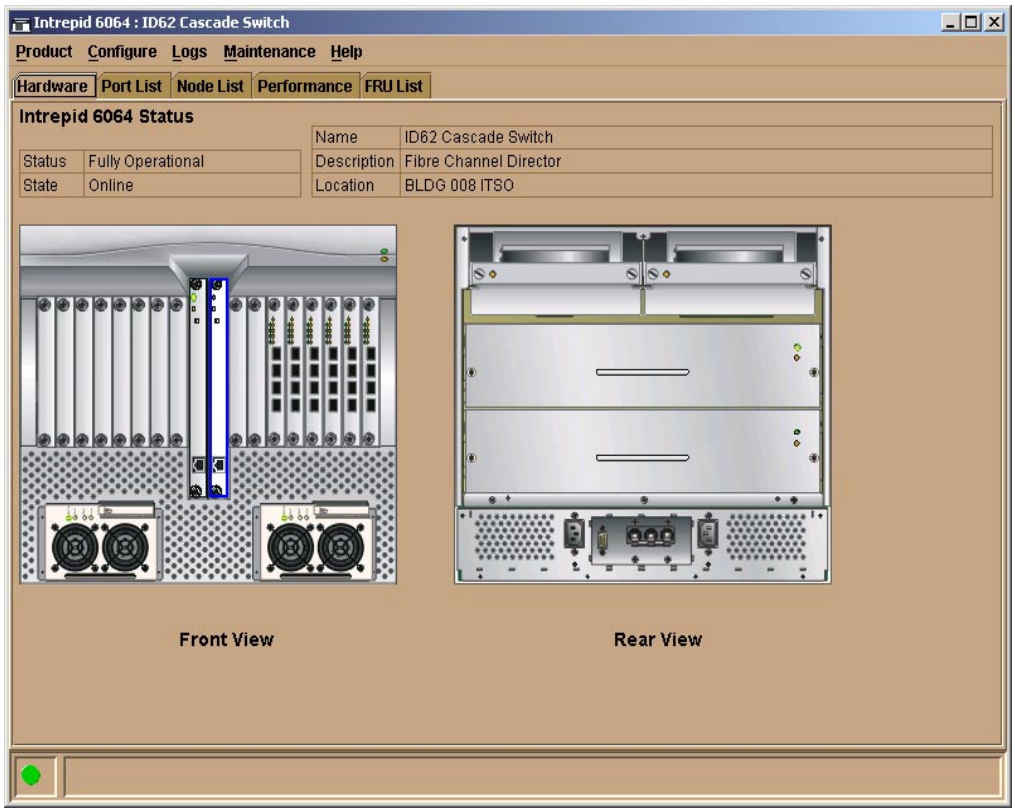


Figure 4-5 Product (Director) display

Product information

Table 4-1 on page 39 lists the various types of information that can be found under the Product information tabs. This information is very useful when configuring the Director, as well as for fault isolation.

Table 4-1 Product information

	Port list	Node list	Performance	FRU list
Port name	X			
Port number (decimal)	X	X	X	
Port address (hexadecimal)	X	X		
Unit type		X		
Alert	X			
FRU type				X

	Port list	Node list	Performance	FRU list
FRU position				X
FRU status				X
FRU serial #				X
FRU part #				X
Block config	X			
Port WWN		X		
Port state	X			
Port speed	X			
Port type	X		X	
B_to_B credit		X		
Port statistics			X	
Link utilization			X	
Error statistics			X	

4.2.2 Fabrics

The Fabrics view displays information about your fabrics, and the Directors and ports within a given fabric (see Figure 4-6).

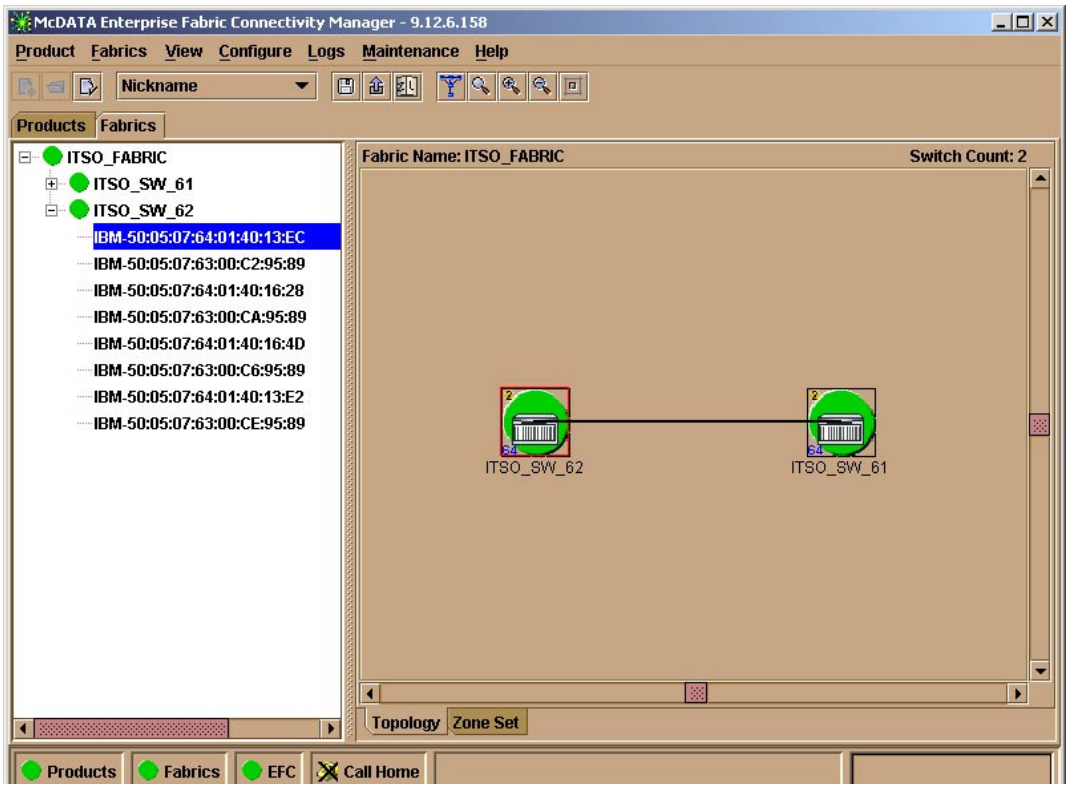


Figure 4-6 Fabric information display

The area to the left is known as the Fabric Tree, and the area to the right is displayed as either the Topology view or the Zone Set view, by selecting tabs at the bottom of the Fabrics view area.

The Topology view shows Directors in fabrics and the Inter-Switch Links (ISLs) between the Directors as solid black lines.

Options available through the menu bar and right-click menus in the Topology view area allow you to manipulate the fabric view, determine routes between Directors, configure fabric-wide zoning, and display fabric, node, and product properties.

4.2.3 Users

This option is located under the Configuration tab, and it allows you to add or delete users. You have to be logged on with a user ID that has *administrator rights* to be able to add or delete a user.

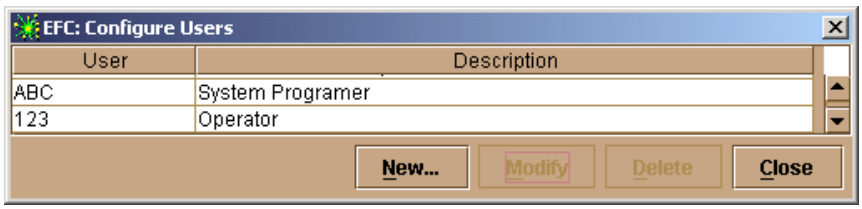


Figure 4-7 Users example

While adding a new user, rights for this user can be selected (see Figure 4-8).The activities of all users can be displayed by the Audit log option.

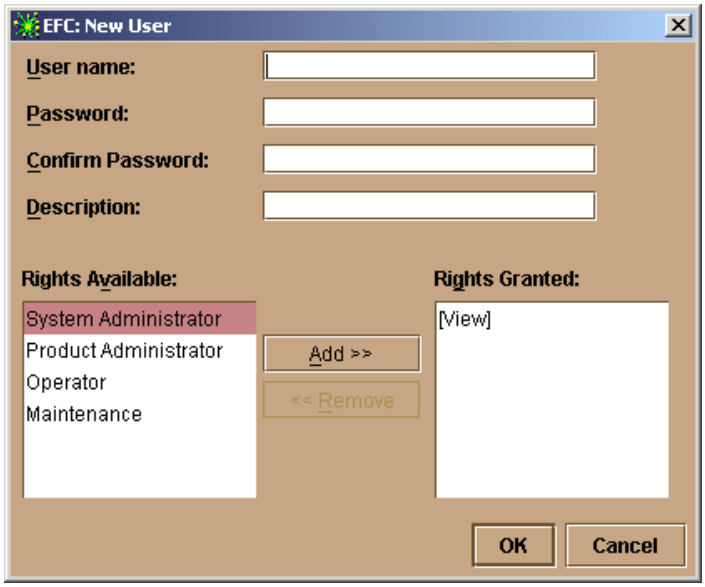


Figure 4-8 New user ID

4.2.4 Logs

Logs are records of events that are stored on the EFC Server's hard drive. Various log types are available under the Logs tab while in Products view or Fabrics view. Each log allows the user to print and/or Export the log. In the following sections are some examples:

Audit log

The Audit log shows a history of all user activities performed through the EFC Manager (see Figure 4-9).

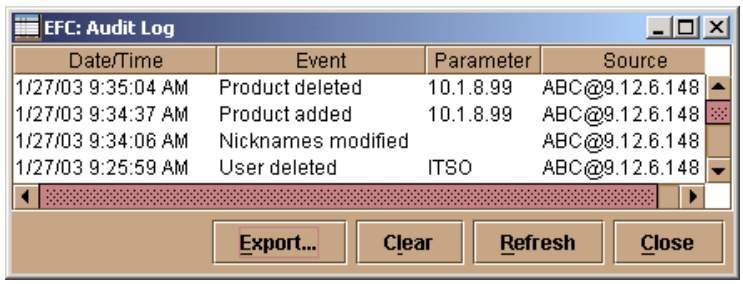


Figure 4-9 Audit log example

Fabric log

The Fabric log shows all changes that occurred to the fabric (see Figure 4-10).

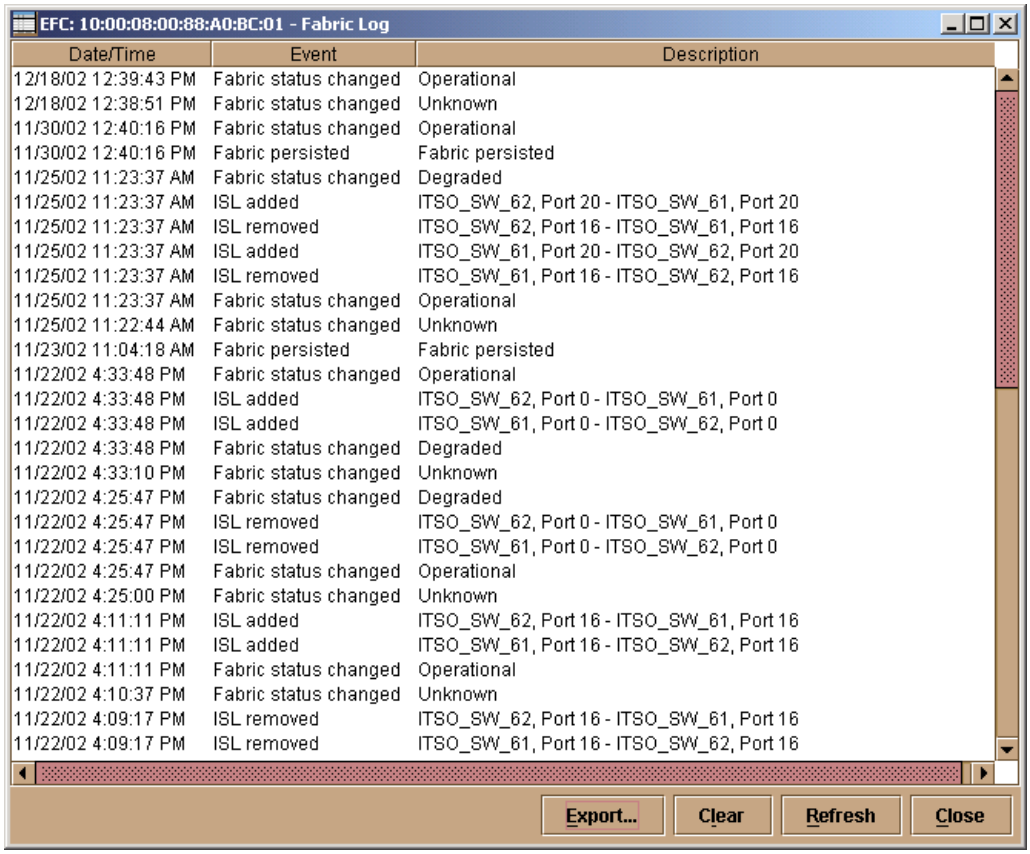


Figure 4-10 Fabric log example

Event log

The Event log provides information about the events in your fabric or products (Directors). See Figure 4-11 for a sample Event log display.

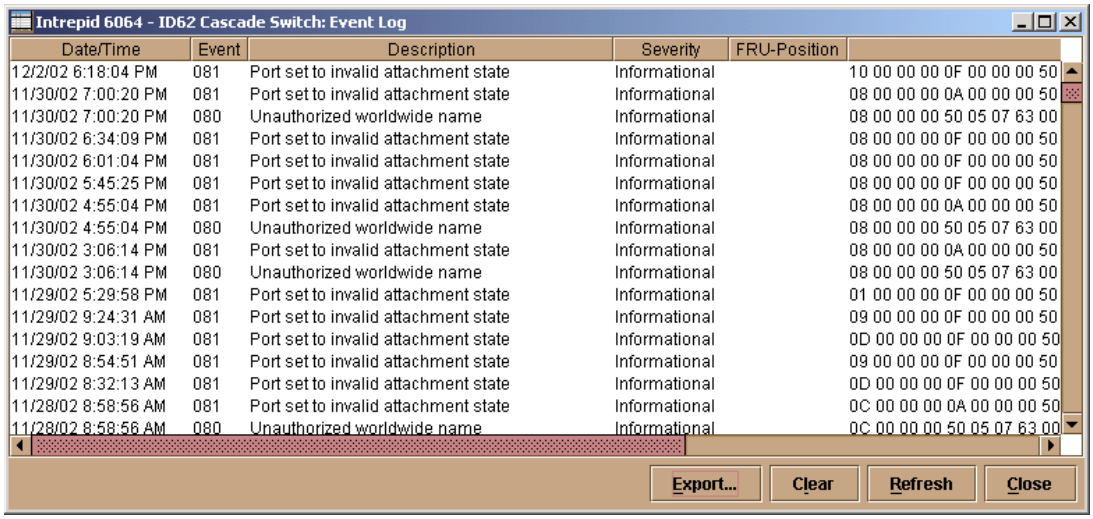

Intrepid 6064 - ID62 Cascade Switch: Event Log
Date/Time Event Description Severity FRU-Position
12/2/02 6:18:04 PM 081 Port set to invalid attachment state Informational 10 00 00 00 0F 00 00 00 50
11/30/02 7:00:20 PM 081 Port set to invalid attachment state Informational 08 00 00 00 0A 00 00 00 50
11/30/02 7:00:20 PM 080 Unauthorized worldwide name Informational 08 00 00 00 50 05 07 63 00
11/30/02 6:34:09 PM 081 Port set to invalid attachment state Informational 08 00 00 00 0F 00 00 00 50
11/30/02 6:01:04 PM 081 Port set to invalid attachment state Informational 08 00 00 00 0F 00 00 00 50
11/30/02 5:45:25 PM 081 Port set to invalid attachment state Informational 08 00 00 00 0F 00 00 00 50
11/30/02 4:55:04 PM 081 Port set to invalid attachment state Informational 08 00 00 00 0A 00 00 00 50
11/30/02 4:55:04 PM 080 Unauthorized worldwide name Informational 08 00 00 00 50 05 07 63 00
11/30/02 3:06:14 PM 081 Port set to invalid attachment state Informational 08 00 00 00 0A 00 00 00 50
11/30/02 3:06:14 PM 080 Unauthorized worldwide name Informational 08 00 00 00 50 05 07 63 00
11/29/02 5:29:58 PM 081 Port set to invalid attachment state Informational 01 00 00 00 0F 00 00 00 50
11/29/02 9:24:31 AM 081 Port set to invalid attachment state Informational 09 00 00 00 0F 00 00 00 50
11/29/02 9:03:19 AM 081 Port set to invalid attachment state Informational 0D 00 00 00 0F 00 00 00 50
11/29/02 8:54:51 AM 081 Port set to invalid attachment state Informational 09 00 00 00 0F 00 00 00 50
11/29/02 8:32:13 AM 081 Port set to invalid attachment state Informational 0D 00 00 00 0F 00 00 00 50
11/28/02 8:58:56 AM 081 Port set to invalid attachment state Informational 0C 00 00 00 0A 00 00 00 50
11/28/02 8:58:56 AM 080 Unauthorized worldwide name Informational 0C 00 00 00 50 05 07 63 00
Export... Clear Refresh Close

Figure 4-11 Event log example

Link incident log

The link incident log displays the most recent link incidents occurring on Director ports. All link incidents are recorded in this log, regardless of whether LIN alerts are configured through the Configure Ports dialog box. See Figure 4-12 for an example of the link incident log.

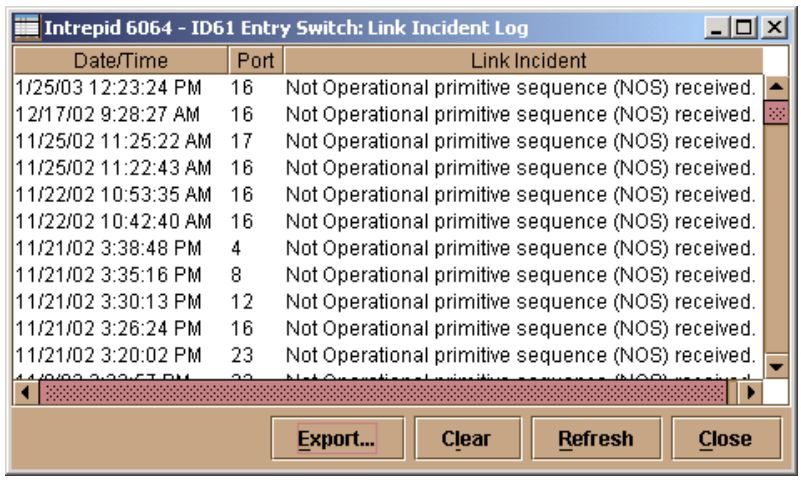

Intrepid 6064 - ID61 Entry Switch: Link Incident Log
Date/Time Port Link Incident
1/25/03 12:23:24 PM 16 Not Operational primitive sequence (NOS) received.
12/17/02 9:28:27 AM 16 Not Operational primitive sequence (NOS) received.
11/25/02 11:25:22 AM 17 Not Operational primitive sequence (NOS) received.
11/25/02 11:22:43 AM 16 Not Operational primitive sequence (NOS) received.
11/22/02 10:53:35 AM 16 Not Operational primitive sequence (NOS) received.
11/22/02 10:42:40 AM 16 Not Operational primitive sequence (NOS) received.
11/21/02 3:38:48 PM 4 Not Operational primitive sequence (NOS) received.
11/21/02 3:35:16 PM 8 Not Operational primitive sequence (NOS) received.
11/21/02 3:30:13 PM 12 Not Operational primitive sequence (NOS) received.
11/21/02 3:26:24 PM 16 Not Operational primitive sequence (NOS) received.
11/21/02 3:20:02 PM 23 Not Operational primitive sequence (NOS) received.
Export... Clear Refresh Close

Figure 4-12 Link incident log example

5

Configuring the FICON Director

This chapter provides information about how to configure the McDATA Intrepid FICON Director in a switched point-to-point configuration or a cascaded FICON Director configuration.

The following topics will be discussed in detail:

- Setting up a FICON Director
- Activating High Integrity Fabric feature
- Enabling the CUP feature
- Building a High Integrity fabric
- Port configuration
- Port WWN Device Names configuration
- Switch Binding
- Zoning
- Verifying the configuration

Note: All tasks described in this chapter require administrator authority. See 4.2.3, “Users” on page 41 for an example.

© Copyright IBM Corp. 2003. All rights reserved.

5.1 Setting up a FICON Director

After installing the FICON Director and establishing connectivity to the EFC Server (as described in Chapter 3, “Pre-installation planning” on page 21), only a few initial steps must be performed.

The following steps are required for each FICON Director, regardless of whether it will be used in a switched point-to-point configuration or cascaded FICON Director configuration, and should be based on your planned configuration:

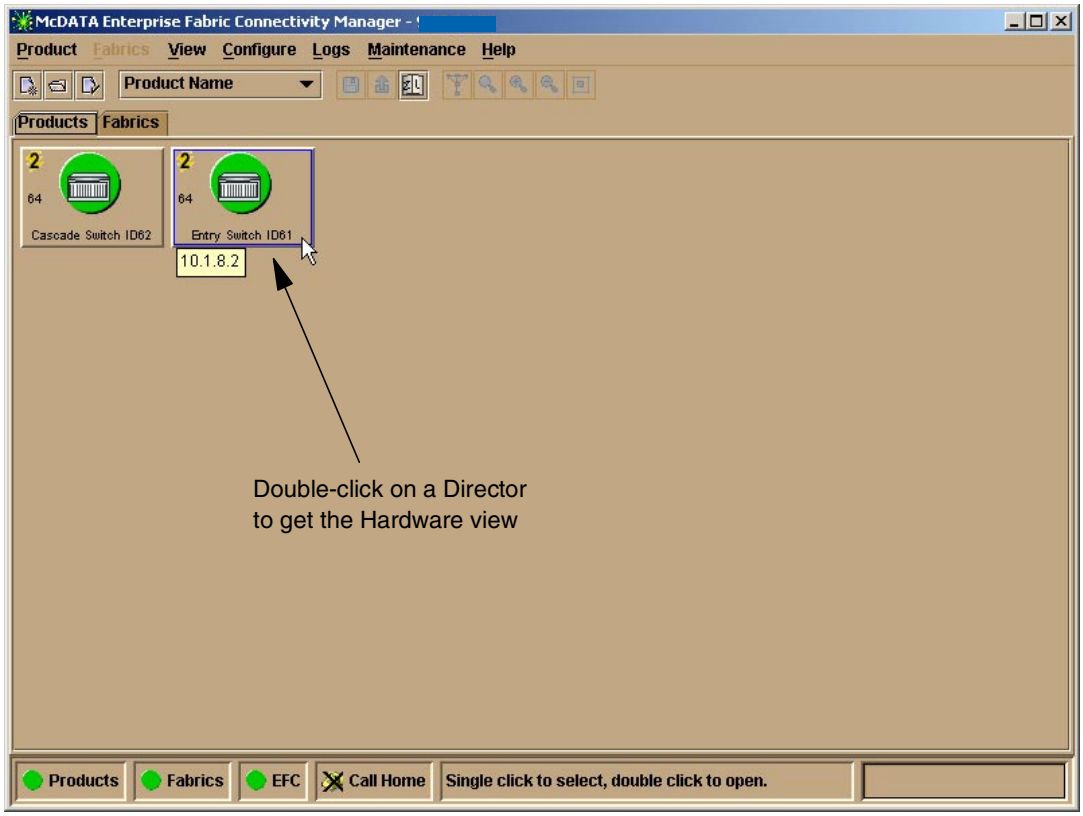


Figure 5-1 Products view of the FICON Directors

1. The Director must be in an offline state to be able to perform the required settings. On the product view screen (which shows all available Directors) double-click the **Director** you want to set up (see Figure 5-1). The next screen is the Hardware view (default display), which provides all option that can be done for the selected Director. From here select the **Maintenance** tab, then from the drop-down select **Set Online State**. Here you can vary the Director offline.

   Figure 5-2 shows the Hardware view of the Director, and that it is now in an OFFLINE state.

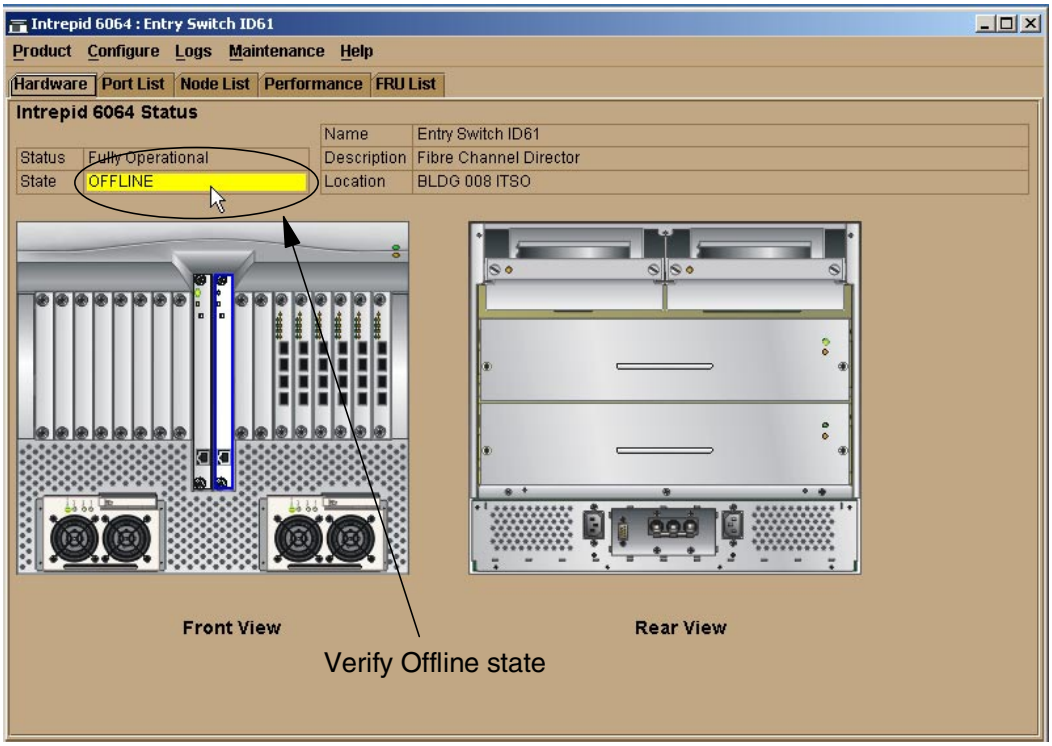


Figure 5-2 Hardware view of the selected Director

2. Click the **Configure tab -> Operating Parameters -> Switch Parameters** (see Figure 5-3).

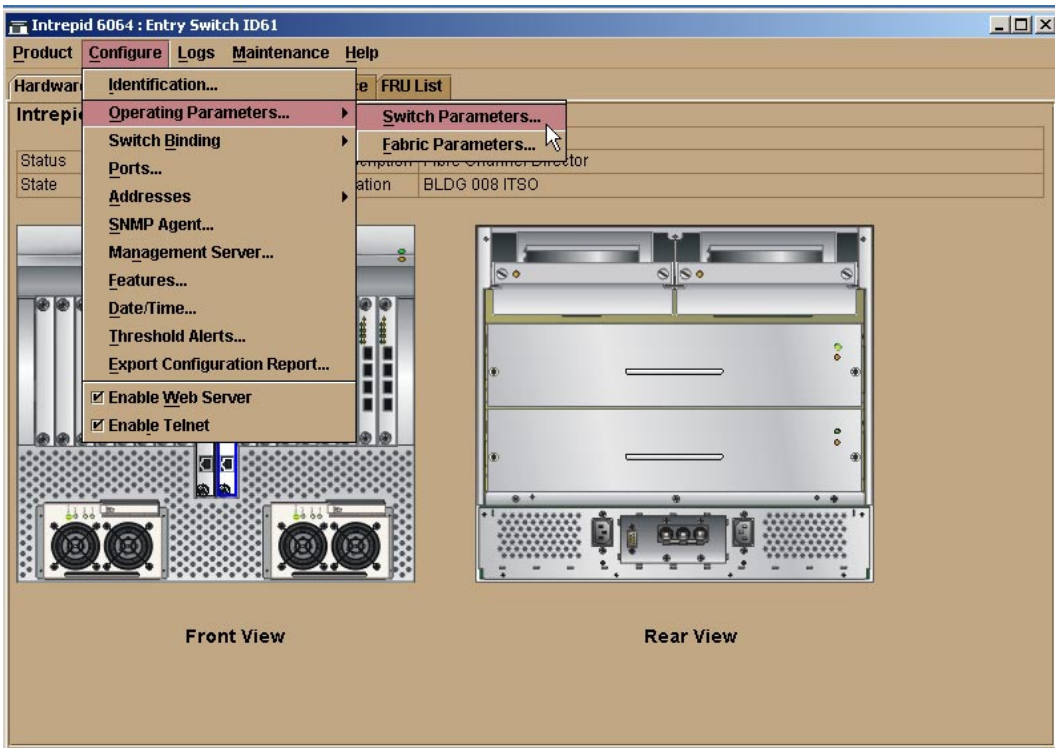


Figure 5-3 Director parameters selection

3. On the Configure Switch Parameters menu perform the following settings:
   - Define preferred *Domain ID*. Notice that each FICON Director must be set up with a unique Domain ID. It is recommended to be the same as the Switch ID used in IOCP/HCD. Enter the required Domain ID into the Preferred field of the menu.

     Entering a 1 into this field results in a Domain ID of x'61" and so on.
   - Check **Insistent** (only if this Director is in a cascaded topology).

     This option is not supported unless the SANtegrity feature is installed (see 5.2, "Activating the High Integrity feature" on page 48).
   - Select **S/390** Operating Mode.
   - From the Director Speed box choose the **2 Gb/sec**.

     Note that the speed for each Director port can be set individually to 1 Gbps, 2 Gbps, or Auto Negotiate from the **Configure -> Ports** list.

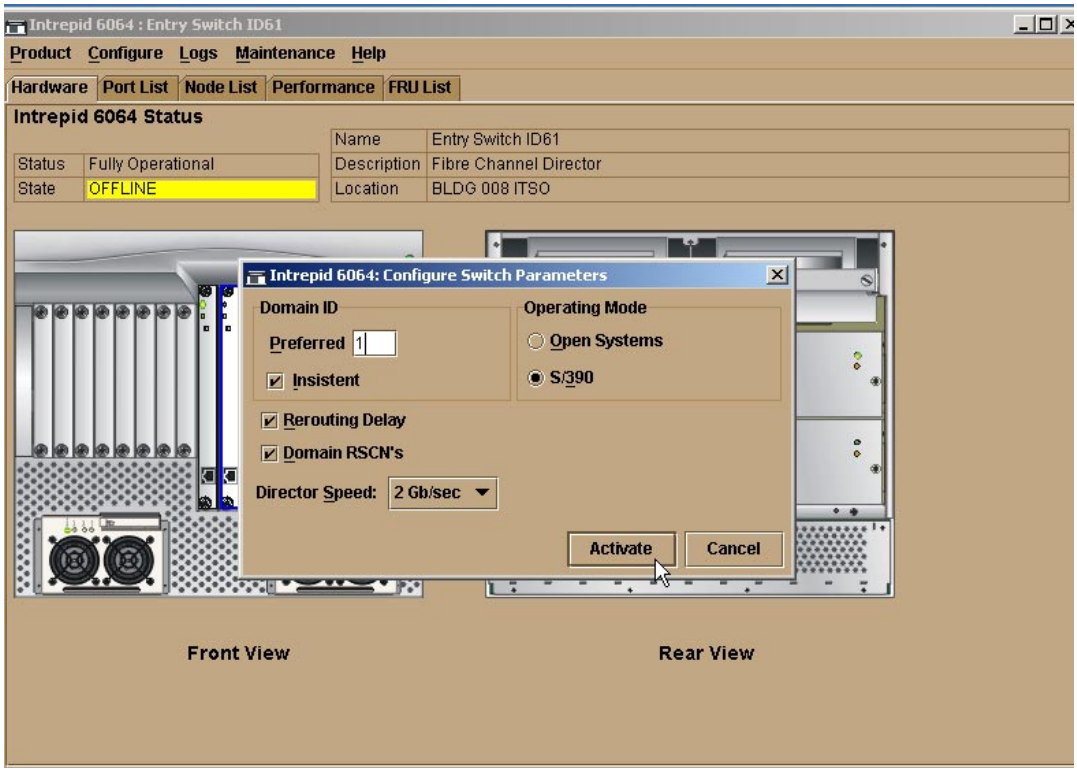


Figure 5-4 FICON Director operating parameters

4. Once the settings are completed, click the **Activate** button, then vary the Director online.

5.2 Activating the High Integrity feature

Establishing a High-Integrity fabric is mandatory for FICON Directors when implemented in a cascaded environment. Both Directors must have the SANtegrity feature installed. The SANtegrity feature is installed by activating the feature key purchased for each Director. The SANtegrity feature (FC 6006 for the Intrepid 6040 or FC 6007 for the Intrepid 6140) is ordered separately.

Important: If the you decide to use 2-byte link addresses in your switched point-to-point configuration, then the Director must have the SANtegrity feature installed. See 3.5, “Binding and Insistent Domain ID” on page 28 for details.

The following steps describe how to activate the SANtegrity feature:

1. Double-click the **Director** to activate the SANtegrity feature. Click the **Configure** tab, then the **Features** option, as shown in Figure 5-5.

   Note: Both FICON Directors must be at the same firmware level before being merged into a High Integrity fabric.

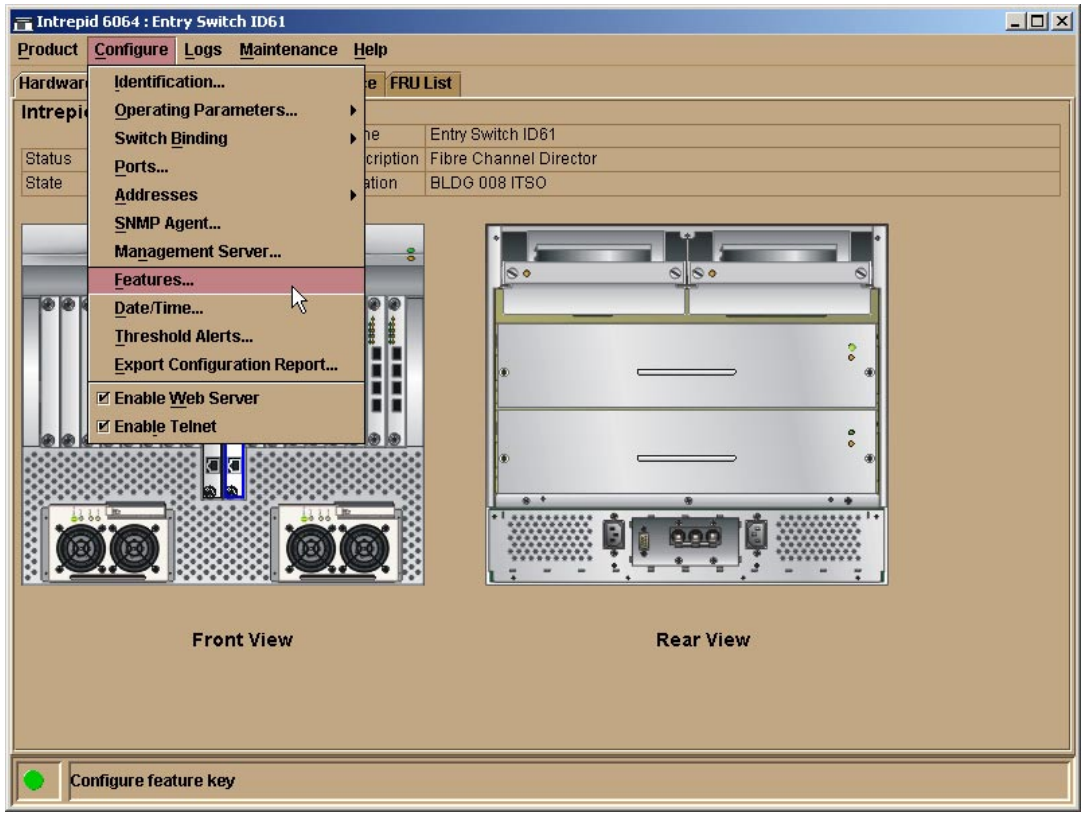


Figure 5-5 Feature key installation

2. On the drop-down select **New,** then enter the feature key in the entry field. Click **OK** (see Figure 5-6).

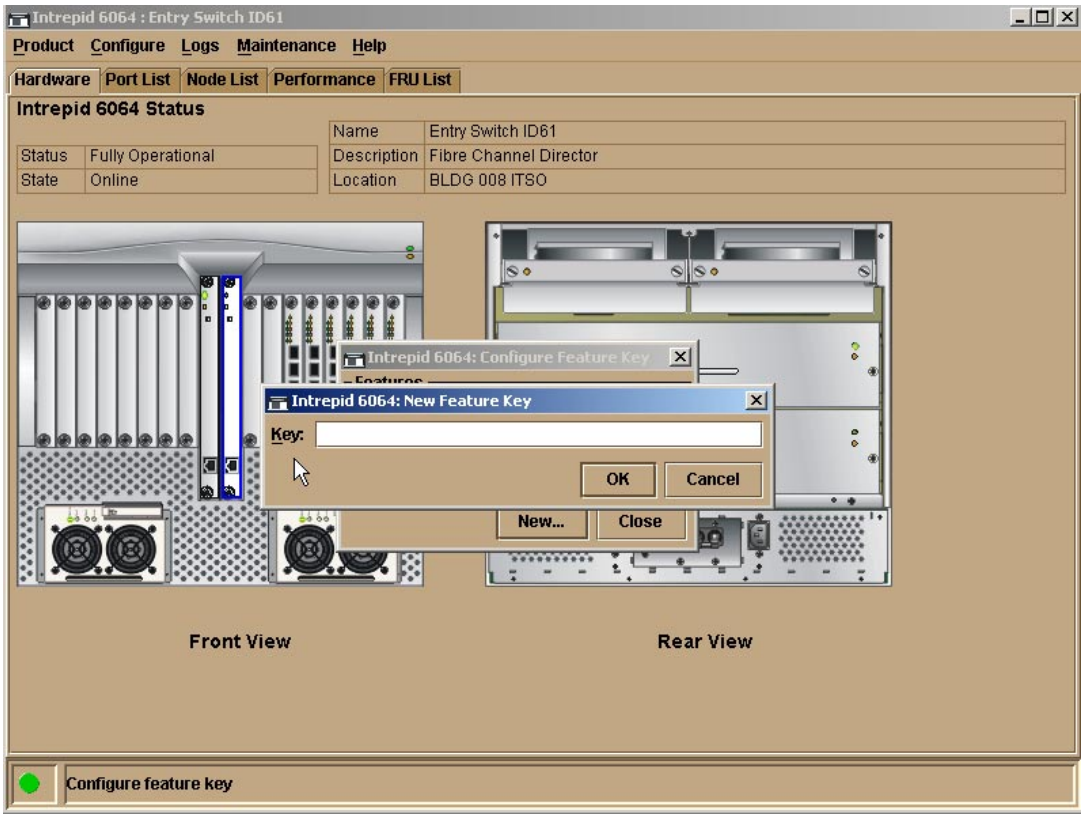


Figure 5-6 Feature Key entry

The installed SANtegrity feature allows E_Port functionality when operating in S/390 mode, which is required for a FICON cascaded topology.

5.3 Enabling the Control Unit Port (CUP)

If the Management Server or CUP feature, FC 6302 (Intrepid 6064) or FC 6003 (Intrepid 6140) has to be activated, these steps have to be performed:

1. Click the **Configuration** tab on the Hardware view, then select **Features**.
2. The Configure Feature Key window is displayed which shows all installed features. If not already in the list, click **New** and enter the McDATA provided key for the FICON Management Server.

   Figure 5-7 shows the window with the installed and enabled features.

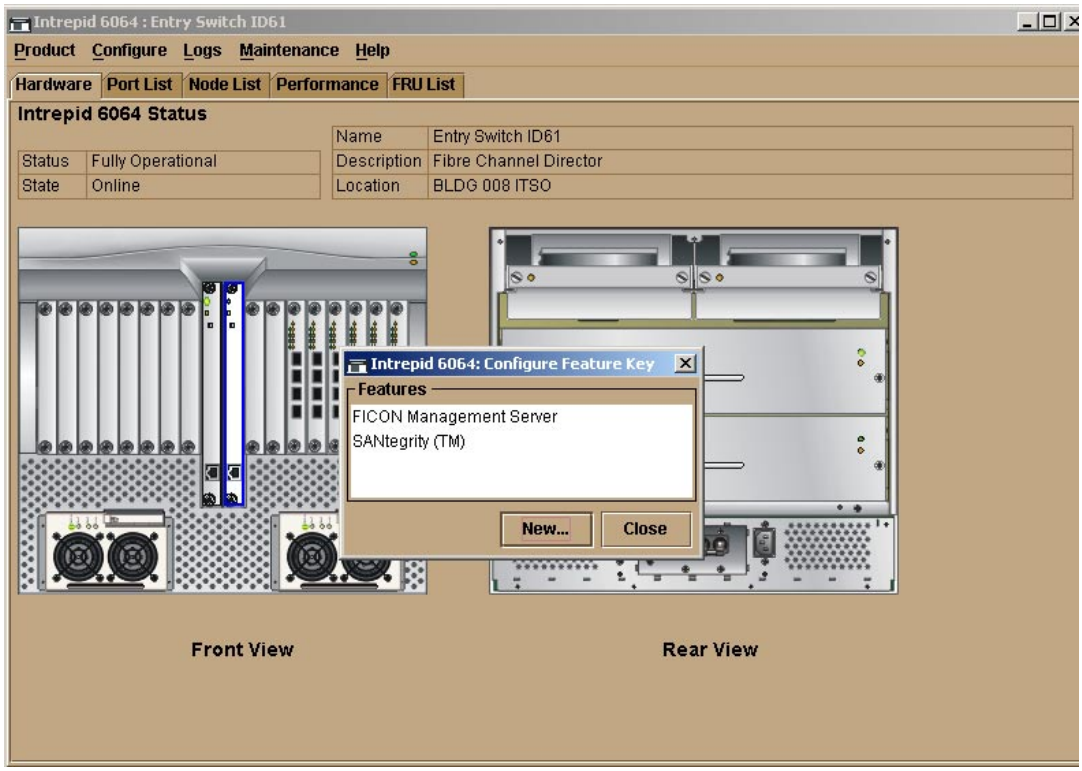


Figure 5-7 List of enabled features

To enable the FICON Management Server feature, do the following:

1. Select **Management Server** from the Configure menu. Enable the management server by clicking the **Enable Management Server** option.

   Note: The following options are not required, and should be set to satisfy your requirements.

2. Click **Director Clock Alert Mode**. If this is enabled, the following occurs when users set the date and time through the Configure Date and Time dialog box.
   - If you enable Periodic Date/Time Synchronization, an error message displays, saying Clock Alert Mode must be cleared to enable automatic date and time synchronization.
   - If you manually set the date and time (Periodic Date/Time Synchronization is not enabled), a confirmation dialog box appears. You must click **OK** on that dialog box to continue manual date and time configuration.
3. Click **Host Control Prohibited** to prohibit a host management program from changing configuration and connectivity parameters on the Director. In this case, the host program has only read access to these parameters. When a check mark is not displayed, the host program can change configuration and connectivity parameters.
4. Click the **Programmed offline state control** to enable a host management program to control the Director offline and online state. When a check mark is not displayed, a host program cannot set the Director online or offline.
5. Click the **Active=Saved** option to enable the active=saved function for the IPL address configuration.

- If **Active=Saved** is enabled (check mark), the IPL and the active address configuration are maintained as identical configurations. If a new configuration is activated through the Configure Addresses - "Active" dialog box, that configuration becomes the IPL address configuration. If the feature is enabled, the IPL file is locked to modification through the Configure Addresses - "Active" dialog box.
- If Active=Saved is disabled (no check mark), the IPL address configuration and the active configuration are not maintained as identical and may, in fact, be different configurations. If the feature is disabled, you can modify the IPL configuration through the Configure Addresses - "Active" dialog box.

6. Select a **code page** from the Code Page list to determine the language for displaying port names or the CUP name when assigned from a host. For example, if the code page for Germany/Austria is selected and a port name is assigned in German by the host management program, then the German language port name appears in the Product Manager.

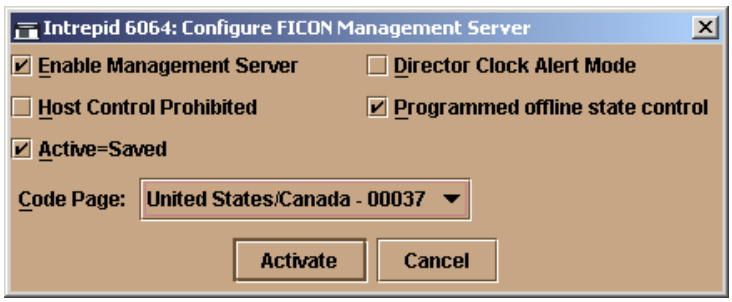


Figure 5-8 Configuring the FICON Management Server

7. Once all required options are set (for example, as in Figure 5-8), click the **Activate** button.

5.4 Building a fabric

To establish a cascaded fabric (two FICON Directors are merged together), several steps are required. Before starting the merging process perform the following:

1. Verify that the appropriate setup has been completed according to the procedure in 5.1, “Setting up a FICON Director” on page 46.

> **Important:** If the Directors are already configured and in use, make sure that **S/390 Operating Mode** is selected. The merge into a cascaded fabric can then be done concurrent to normal operation.

2. Double-click the first **Director**, which will be part of the fabric, then click **Configure, Operating Parameters, Fabric Parameters**.
3. Check the following settings as shown in Figure 5-9:
   - The BB_Credit can be between 1 and 60 buffers. This becomes the value for all ports, except those configured for extended distance buffering (10-100 Km). The default value is 16.
   - The R_A_TOV and E_D_TOV time-out values must be the same for both Directors, otherwise they cannot be merged into a cascaded fabric.
   - McDATA Fabric 1.0 is the Interop Mode used, since a cascaded FICON configuration requires that both Directors must be from the same vendor.

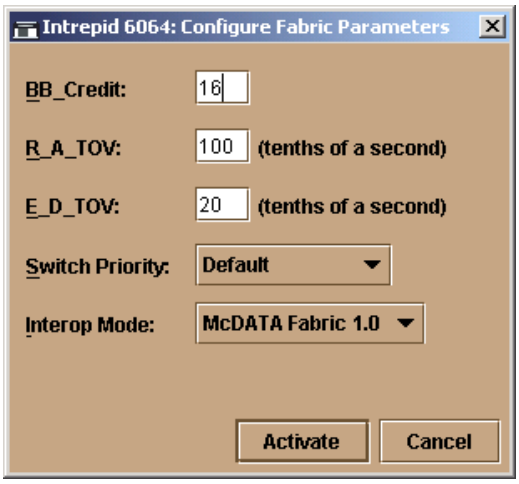


Figure 5-9 Verify settings of FICON Directors

We used the default values for our configuration. However, the BB_Credit was changed for certain ports when we enabled long distance buffering, as shown in 5.5.3, “Configuring a port” on page 61.

4. Verify/apply settings on the second Director that will be included in the fabric.

If you wish to use Switch Binding, ensure all the devices are attached to the Directors. The devices (WWNs) are automatically placed in the Switch Binding membership list when Enterprise Fabric Mode is enabled. Switch Binding is described under 5.4.1, “Switch Binding” on page 56.

5. Identify and connect the ISLs based on your configuration requirements.

Note: Blocking the E_Ports used for ISLs is recommended when connecting the ISLs between the Directors. This ensures that the fabric remains stable during the cabling process. Unblock the ports one-by-one after connecting the cables, and check for errors in the logs (see “Fabric log” on page 42, “Event log” on page 42, and “Link incident log” on page 43).

Activating Enterprise Fabric Mode enables the features (Fabric Binding and Insistent Domain ID), necessary to support FICON cascaded Directors.

6. Select **Fabrics** from the Products view screen and choose **Enterprise Fabric Mode** as shown in Figure 5-10.

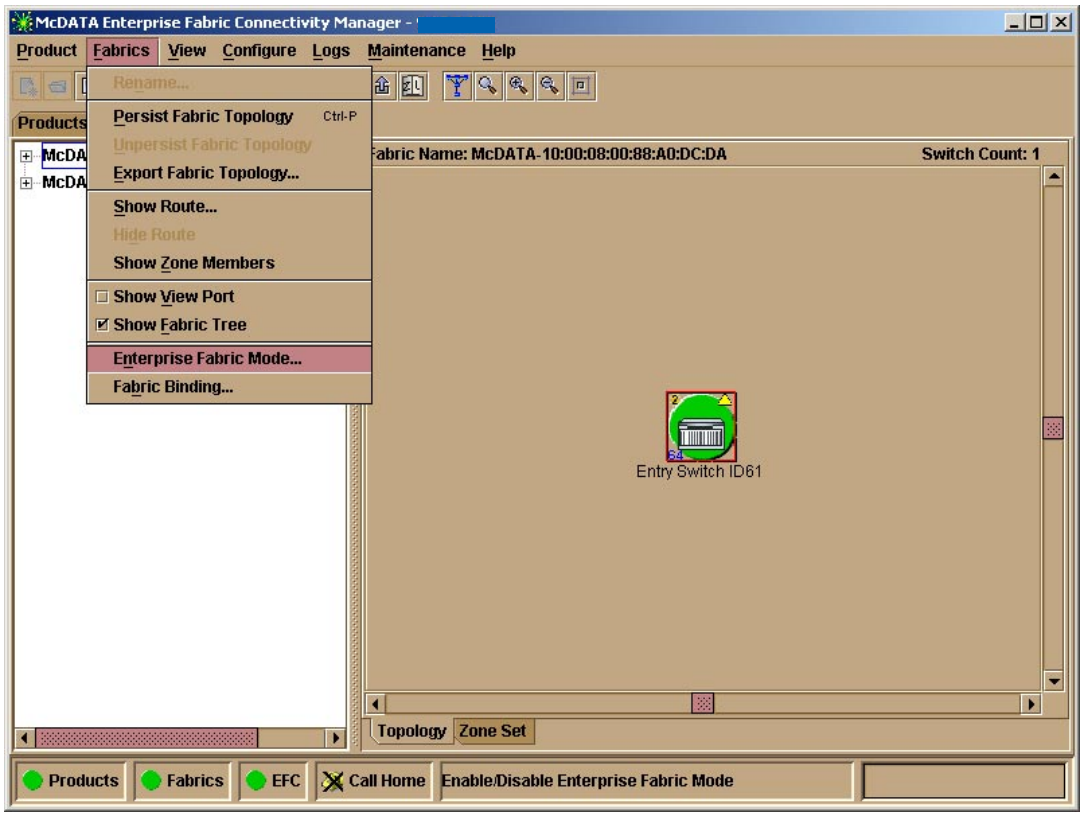


Figure 5-10 Enterprise Fabric Mode

7. Click **Start**. This enables all listed features as shown in Figure 5-11. Ensure the operation completes successfully, which indicates Enterprise Fabric is established.

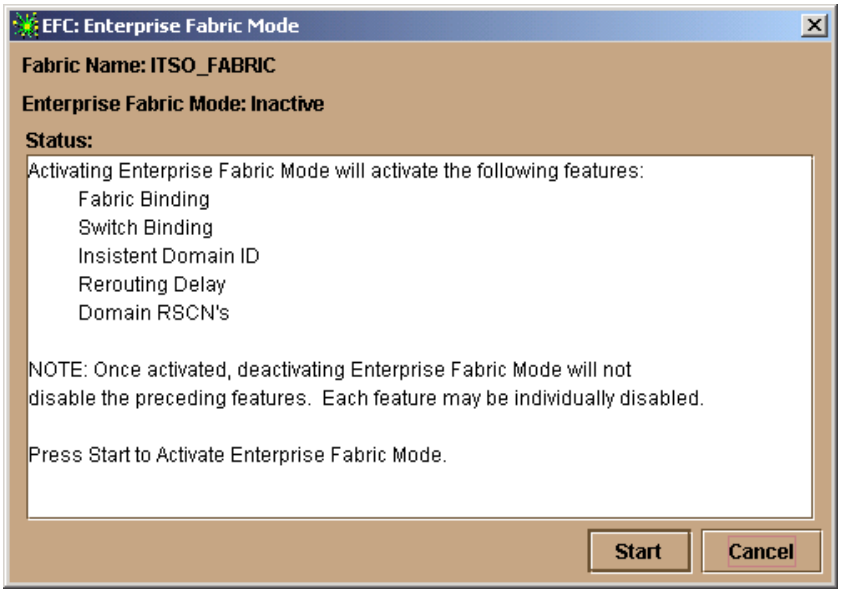

EFC: Enterprise Fabric Mode
Fabric Name: ITSO_FABRIC
Enterprise Fabric Mode: Inactive
Status:
Activating Enterprise Fabric Mode will activate the following features:
Fabric Binding
Switch Binding
Insistent Domain ID
Rerouting Delay
Domain RSCN's
NOTE: Once activated, deactivating Enterprise Fabric Mode will not
disable the preceding features. Each feature may be individually disabled.
Press Start to Activate Enterprise Fabric Mode.
Start
Cancel

Figure 5-11 Features enabled with Enterprise Fabric Mode

8. After clicking **OK** to enable Enterprise Fabric Mode, wait for the message: `Enterprise Fabric Mode update complete`, then click the **Close** button to finish.

When Enterprise Fabric Mode is activated, a fabric membership list is automatically created containing the Domain ID and WWN of both Directors.

9. Verify the membership list by selecting **Fabrics -> Fabric Binding -> Next -> Membership** list. The list is shown in Figure 5-12.

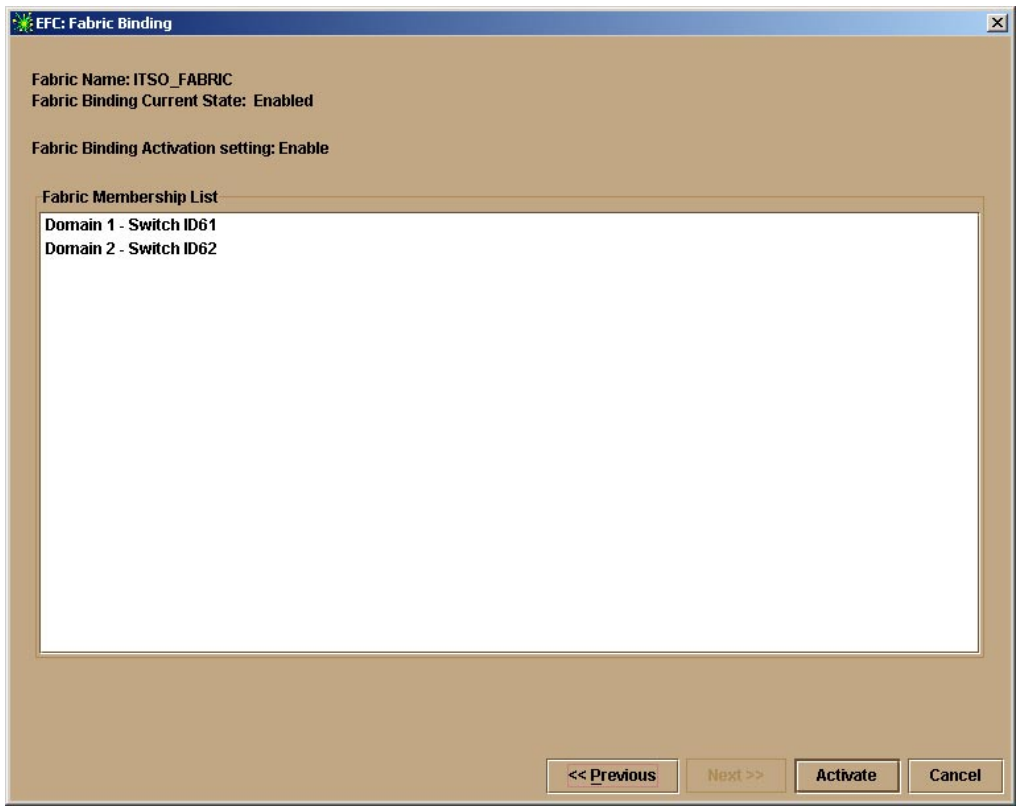


Figure 5-12 Membership List containing Directors included in the fabric

Note: If any Director that is not in the membership list is connected to this Director, the ISL link will segment. An “invalid attachment” is reported on the isolated E_Port.

10. After verifying the fabric settings, change to the Fabrics view, which will show the complete fabric as seen in Figure 5-13. Right-click the **ISL** to display details about ISL connection.

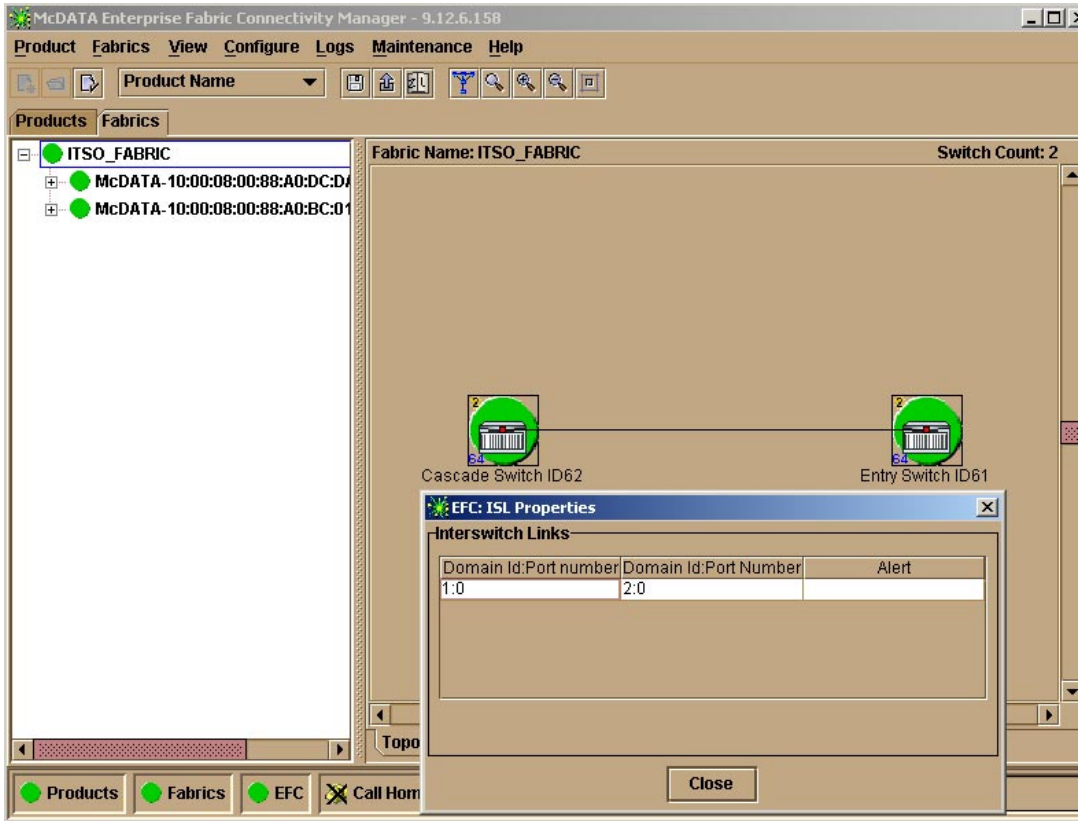


Figure 5-13 Established fabric with ISL link

5.4.1 Switch Binding

If additional security is required, Switch Binding can be established to allow only specific devices (based on WWN or Nickname) to connected to a Director.

As mentioned earlier, all devices which were connected during the Enterprise Fabric Mode enabling process will be automatically put into the membership list for Switch Binding. You can add devices at any time using the **Configuration** tab for a selected Director, or by using the **Edit Membership List** option (see Figure 5-14).

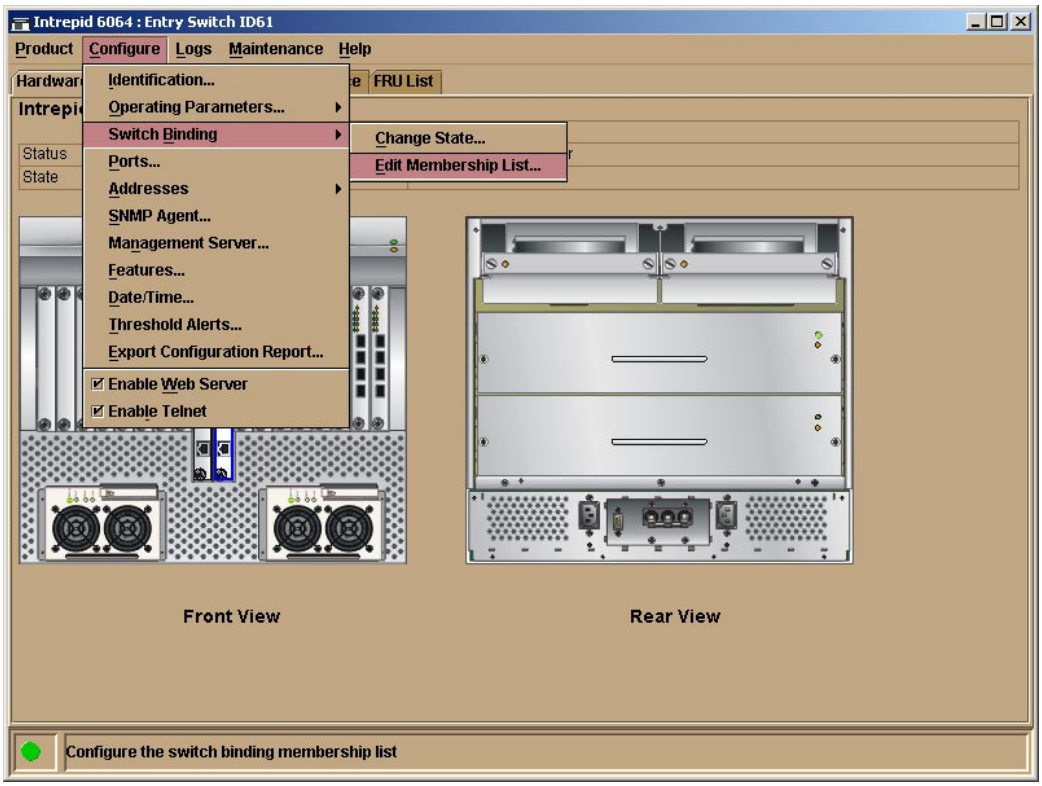


Figure 5-14 Switch Binding selection

Figure 5-15 shows a membership list for Switch Binding. You can add or delete devices based on WWN or Nicknames. A check box indicates if the devices are in the membership list.

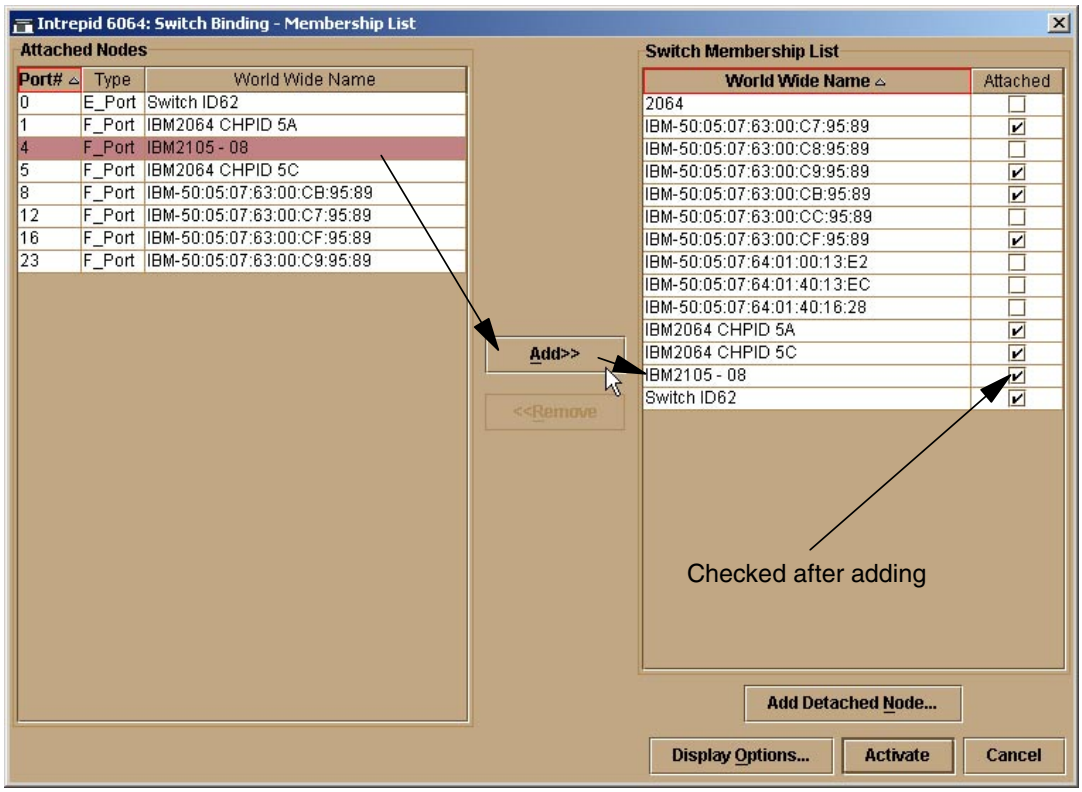


Figure 5-15 Add device to Switch Binding membership list

The last step is to activate the changes by selecting the **Activate** button.

To remove a device from the list, Switch Binding must first be disabled.

Note: Switch Binding cannot be disabled while Enterprise Fabric Mode is active and the Director is online.

5.5 Port configuration

This section describes how to configure ports, port names, port binding, port type, port speed, blocked or unblocked, state and enable, or disable long-distance buffering.

5.5.1 Defining Nicknames

Each port is initially identified by a WWN, which is an 8-byte hexadecimal number. Assigning a meaningful Nickname to a port or node makes it easier to identify a device when it is connected to the port:

1. In the EFC Manager window double-click the icon of the **Director** where you want to configure the ports.
2. A new window opens displaying the Hardware view of the Director. Click the **Node List** tab. A list of all connected devices is displayed as shown in Figure 5-16. The WWN and the Unit Type are automatically retrieved from the device connected to the port.

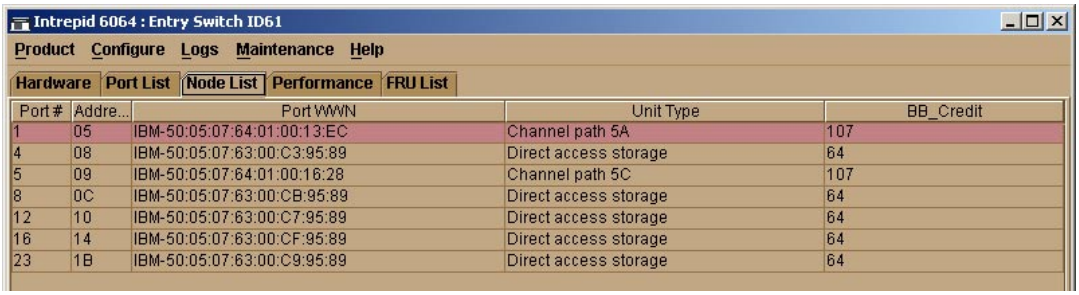

Intrepid 6064 : Entry Switch ID61
Product Configure Logs Maintenance Help
Hardware Port List Node List Performance FRU List
Port # Addre... Port WWN Unit Type BB_Credit
1 05 IBM-50:05:07:64:01:00:13:EC Channel path 5A 107
4 08 IBM-50:05:07:63:00:C3:95:89 Direct access storage 64
5 09 IBM-50:05:07:64:01:00:16:28 Channel path 5C 107
8 0C IBM-50:05:07:63:00:CB:95:89 Direct access storage 64
12 10 IBM-50:05:07:63:00:C7:95:89 Direct access storage 64
16 14 IBM-50:05:07:63:00:CF:95:89 Direct access storage 64
23 1B IBM-50:05:07:63:00:C9:95:89 Direct access storage 64

Figure 5-16 Node List WWN display

3. Right-click the port and select **Define Nickname...** from the menu. In the Define Nickname window, the WWN of the device is shown, and there is a blank field to enter the nickname for the device. See the example in Figure 5-17.

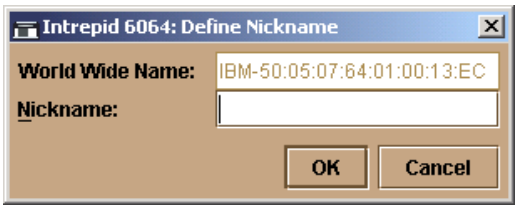


Figure 5-17 Enter Device nick Name

4. In the Nickname field, type in a meaningful Nickname describing the device connected to the port.

Attention: Nicknames must be unique within the Director.

5. Repeat above steps for all devices connected to the switch. The Node List shows the Nickname in the WWN column instead of the WWN. See the example in Figure 5-18.

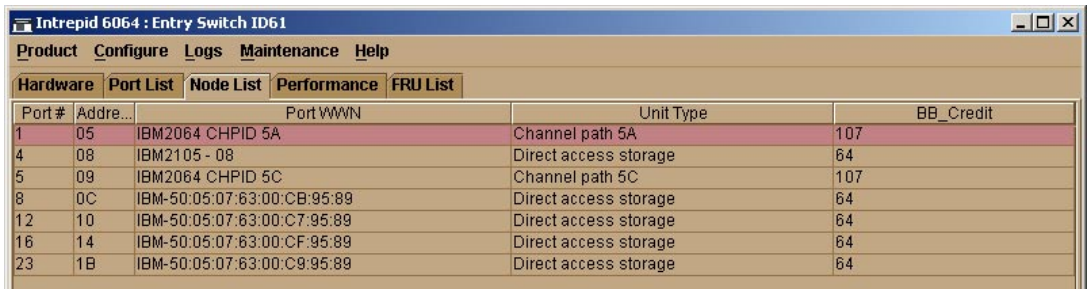

Intrepid 6064 : Entry Switch ID61
Product Configure Logs Maintenance Help
Hardware Port List Node List Performance FRU List
Port # Addre... Port WWN Unit Type BB_Credit
1 05 IBM2064 CHPID 5A Channel path 5A 107
4 08 IBM2105 - 08 Direct access storage 64
5 09 IBM2064 CHPID 5C Channel path 5C 107
8 0C IBM-50:05:07:63:00:CB:95:89 Direct access storage 64
12 10 IBM-50:05:07:63:00:C7:95:89 Direct access storage 64
16 14 IBM-50:05:07:63:00:CF:95:89 Direct access storage 64
23 1B IBM-50:05:07:63:00:C9:95:89 Direct access storage 64

Figure 5-18 Display Nicknames in the WWN column

If it is necessary to display the WWN of a device, right-click any **port,** then select **Display Options** and **World Wide Name** from the menu. The WWN of the devices appear in the Port WWN column.

5.5.2 Defining port names and blocking ports

While the Nicknames entered in the Node List belong to the devices connected to the Director, the ports in the Director will have there own names for describing the port:

1. From the Hardware view of the Director, click **Configure - Addresses - Active...** (see Figure 5-19).

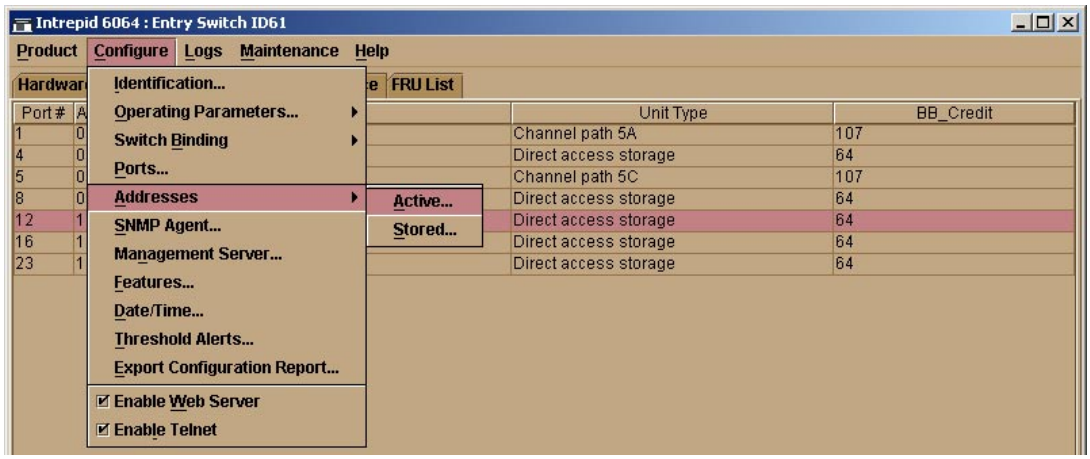


Figure 5-19 Configure dialog menu

2. The Configure Addresses panel opens. On this panel you can enter your port names, block ports, and prohibit communication between ports if required. To enter a name for a port double-click the **Port Name** field of the port.
3. Type in a meaningful name for that port in the Port Name field.
4. Click i the check box in the **Blocked** column if you want to block a port. Blocked ports still transmit offline sequences (OLS), but can not communicate to an attached device.
5. Prohibit port-to-port communication (if required). Click the **intersection of the ports** in which you want to prohibit communication.

See Figure 5-20 for an example of port names, blocked ports, and prohibited port-to-port communication.

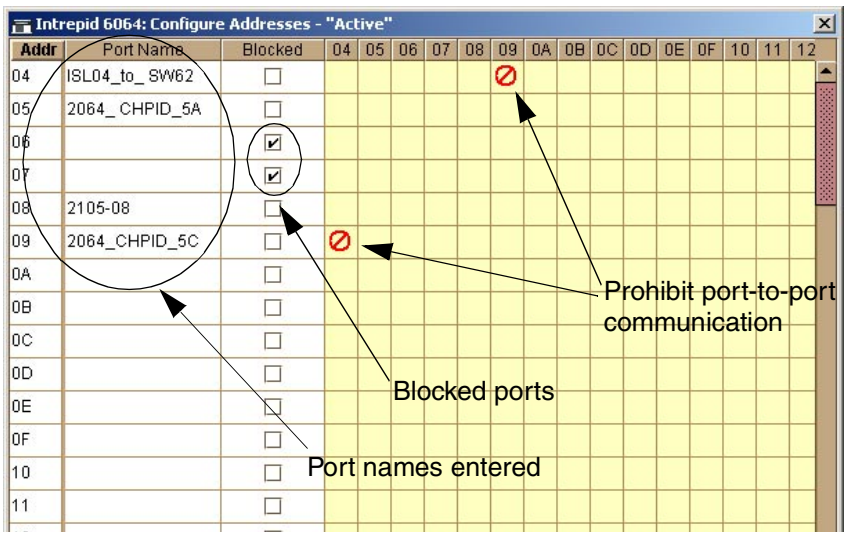


Figure 5-20 Configure Addresses panel

In this example, several port names are entered, ports 06 and 07 are blocked, and communication between port 04 and 09 is suppressed.

5.5.3 Configuring a port

This section describes how to configure port options such as, long distance buffering, port binding, and speed.

If the 10-100 km feature is enabled, more buffer-to-buffer credits are provided to a port in support of long distance links. The speed for each port should be set to the speed supported by the attached device:

1. Click **Configure** from the Products view of a Director, then select **Ports** from the menu.

   The Configure Ports panel is displayed, as shown in Figure 5-21.

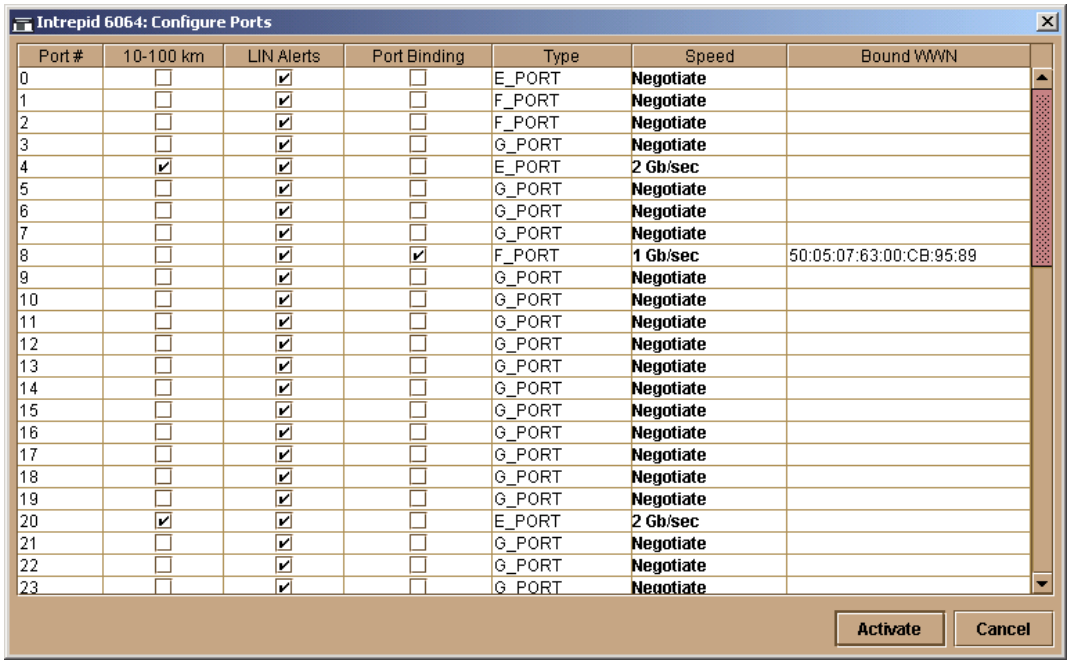


Figure 5-21 Configure ports

2. Check the check box in the 10-100 km column for ports that require the long distance feature.

   With this option, the buffer-to-buffer credit will automatically to changed to 60 for the port, overriding the buffer-to-buffer credit defined for the Director, as shown in 5.4, “Building a fabric” on page 52.

3. If the speed of the port should not be negotiated, click the **Speed** field of a given port and select the speed from the pull-down.

4. If port binding is required, click the **check box** and add the WWPN of the device in the Bound WWN field that will be attached to that particular port.

5. Once all ports are configured, click the **Activate** button to activate and save changes.

5.6 Zoning

Zoning is required to group several ports or WWNs into a zone. Several zones can be created holding different ports or WWNs. All zones are then grouped into a zone set. The zone set has to be activated in a Director, and is automatically propagated to all other Directors in the fabric.

5.6.1 Creating a zone

1. From the Fabrics view (as shown in Figure 5-22 on page 62), do the following:

   ❶ Select **Fabrics**.

   ❷ Select **Zone Set**.

   ❸ Select **Configure**.

   ❹ Select **Zoning Library...**

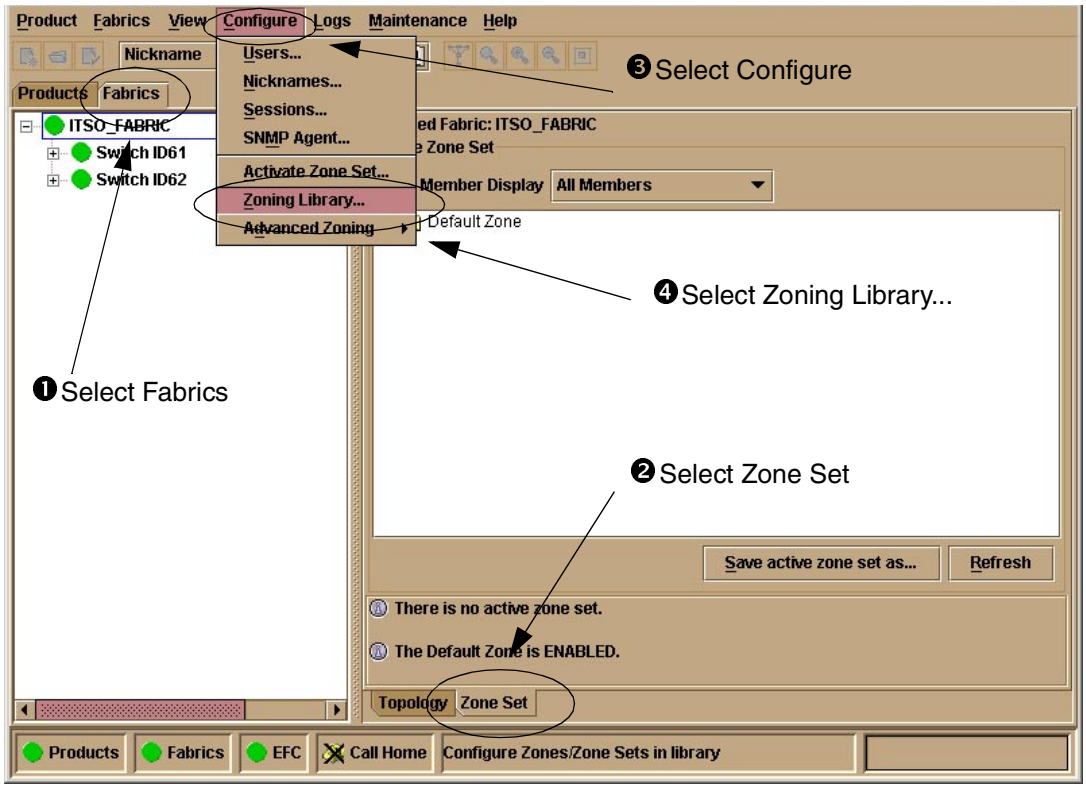


Figure 5-22 EFC Manager Zoneset display

Initially, the Zoning Library window (shown in Figure 5-23), will have no zone sets nor zones listed.

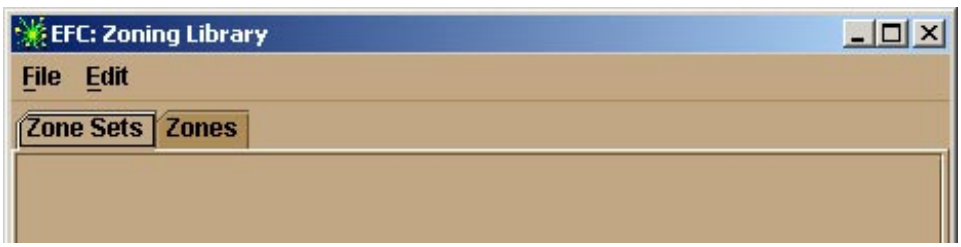


Figure 5-23 Zoning Library

2. Click on the **Zones** tab, then on **File - New** to create a new Zone.

   In the next window all Directors belonging to the selected fabric and their attached ports are shown in the left-hand column. To select another fabric click the **Fabric** pull-down menu to choose another fabric.

On the New Zone window shown in Figure 5-24 do the following to add new members to the zone:

❶ Type in a name for this zone. A zone name may have up 64 characters.

❷ Choose the option to add members by WWN or by Port. If **Add by WWN** is selected and a nickname for this port has been previously defined, the nickname is displayed.

❸ Click the **port** you want to add to the zone.

❹ Click the **Add>>** button to get the selected port into the member list in the right column.

❺ The port just added should now appear in the member list in the right column.

Repeat above steps for all ports you want to group into the zone.

Restriction: A zone can group up to a maximum of 4096 members.

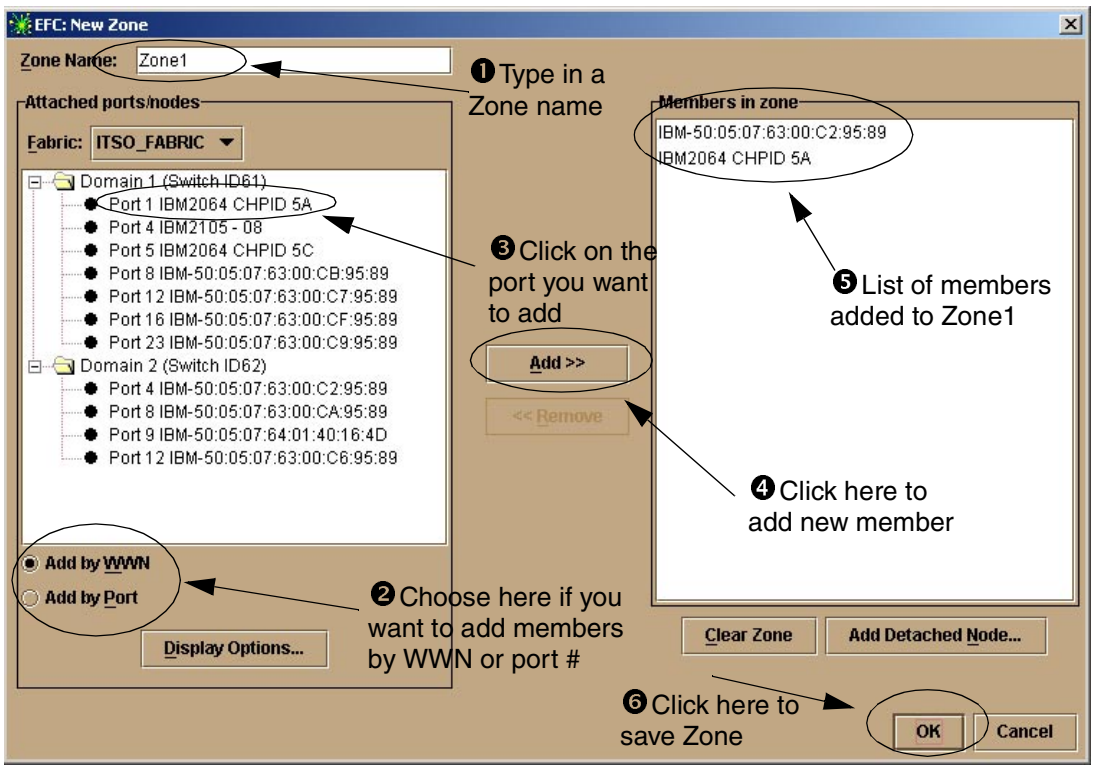


Figure 5-24 Define New Zone

3. Once all ports have been put into the zone, check the member list in the right column for completion. In the example above, two ports are added to the member list for Zone1.

   ❻ Click **OK** to save the zone.

Repeat above steps to create more zones and add members to the zone as required.

Restriction: A maximum of up to 1024 zones can be defined in zone set.

5.6.2 Creating a zone set

Zones created in the previous section are grouped into Zone Sets. Although, several zone sets can be created to group zones, only one zone set can be active at a time. A maximum of

64 zone sets can be defined in the zoning library and each zone set can group up to 1024 zones.

1. In the *Zoning Library* window (see Figure 5-23) click the **Zone Sets** tab.
2. On the menu bar, click **File - New...** to open the New Zone Set window.

   All zones defined in the zoning library are listed in the left column. See Figure 5-25 for the New Zone Set screen.
3. Type a name for the zone set. The name can have a maximum of 64 characters; then click the **zone** you want to add to the zone set.
4. Click the **Add** button to add the zone into the right column.

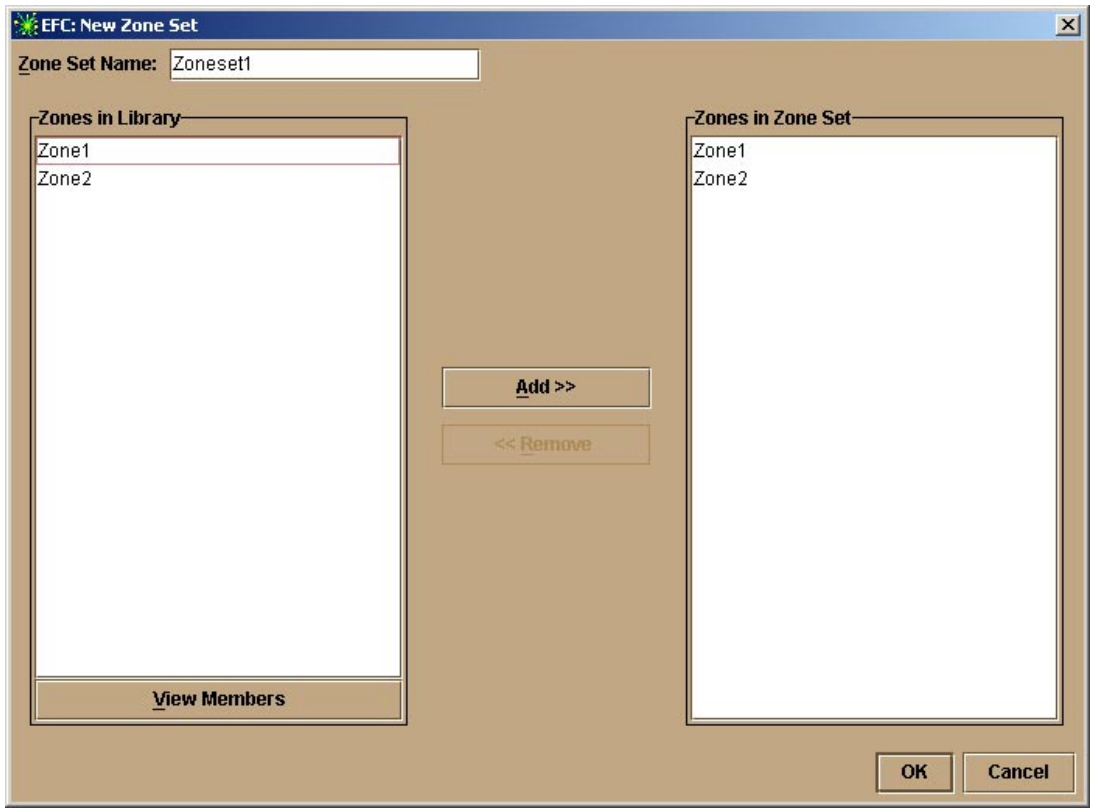


Figure 5-25 Create a zoneset

To verify that the right zone is selected for adding to the zone set, click the **zone**, and then click **View Members**. This shows the members belonging to that specific zone.

5. Once all the zones grouped into the zone set are added to the right column, click the **OK** button to save this zone set.
6. Now you have a new zone set in the zoning library. See Figure 5-26 for a sample zone set in the zoning library.

Figure 5-26 Zonesets in zoning library

Restriction: Up to 64 zone sets can be defined in the zoning library.

To verify that zones and zone members are correctly added to the zone set, click the **zone set** and select **File - Properties** from the menu bar. The complete zone set members and the zone members are displayed, as shown in Figure 5-27.

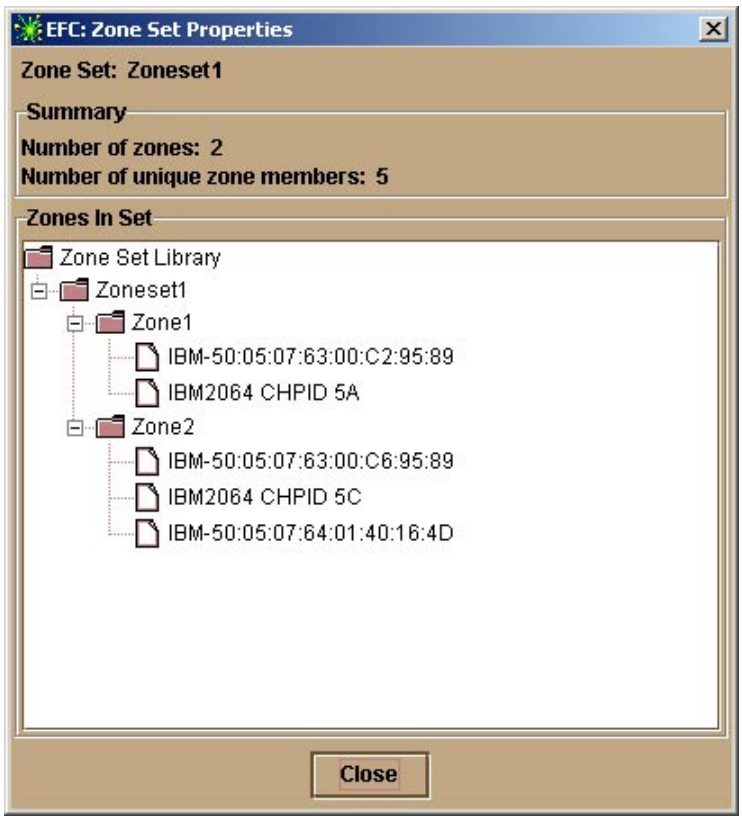


Figure 5-27 Zoneset properties

Once all your zone definitions are correct, close the zone set properties window.

5.6.3 Activating a zone set

Several zone sets can exist in the zoning library and can be activated any time. There is one zone which cannot be defined manually, that is the *default zone*. All ports not being grouped into the current active zone are automatically grouped into the default zone. If no zone set is active, then all devices belong to the default zone.

Important: If you deactivate the active zoneset and the default zone feature is enabled, then all nodes in the fabric will be able to communicate with all other nodes. This could in turn lead to violations of your security policies.

If you want to disable the default zone feature, select **Configure - Advanced Zoning - Configure Default Zone** from the menu bar. On the next panel you can enable or disable the default zone feature.

It is not necessary to deactivate the current active zoneset. Activation of a new zoneset replaces the current active zone set. Deactivating the current active zone set causes the default zone to be activated if the default zone feature is enabled.

To deactivate the current zone set, select from the menu bar **Configure - Advanced Zoning - Deactivate Zone Set.** On the next panel click the **Start** button to deactivate the current zone set and update the fabric.

At installation time there is no current active zone set. To activate a zone set, do the following:

1. In the EFC Manager window click the **Fabrics** tab.
2. Click the **Zone Set** tab.
3. Select **Configure** on the menu bar.

See Figure 5-28 for an example of the above steps.

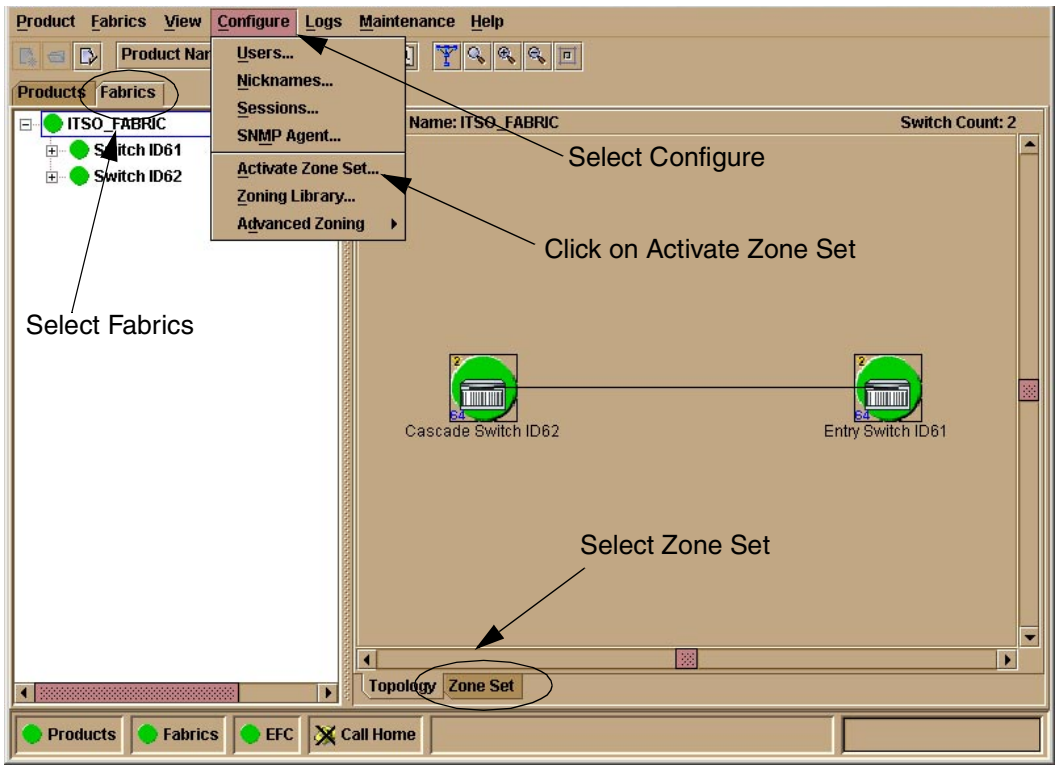


Figure 5-28 Activate Zone Set

4. On the pull-down, click **Activate Zone Set...**
5. The next screen shows a list of all defined zone sets. Select a **zone set** from the list, then click **Next**.

6. On the next screen the name of the fabric and a list of the affected Directors is displayed. Ensure you have chosen the correct fabric and Directors for zone set activation. Applying the zoneset to an other fabric may impact the performance of these switches.
7. Click **Next** and **Start** to continue the zoneset activation, and wait for message: `Activate zone set complete`, then close the window.
8. On the EFC Manager window click the **Zone Set** tab.

   The current active zone set and the zone members are listed in the window. An example of an activated zone set is shown in Figure 5-29.

   In this example Zoneset1 is the current active zone set. Zone1 and Zone2 are assigned to Zoneset1 and the members of these zones are listed.

   Because some of the devices are not defined in any of the zones, they are automatically grouped into the default zone.

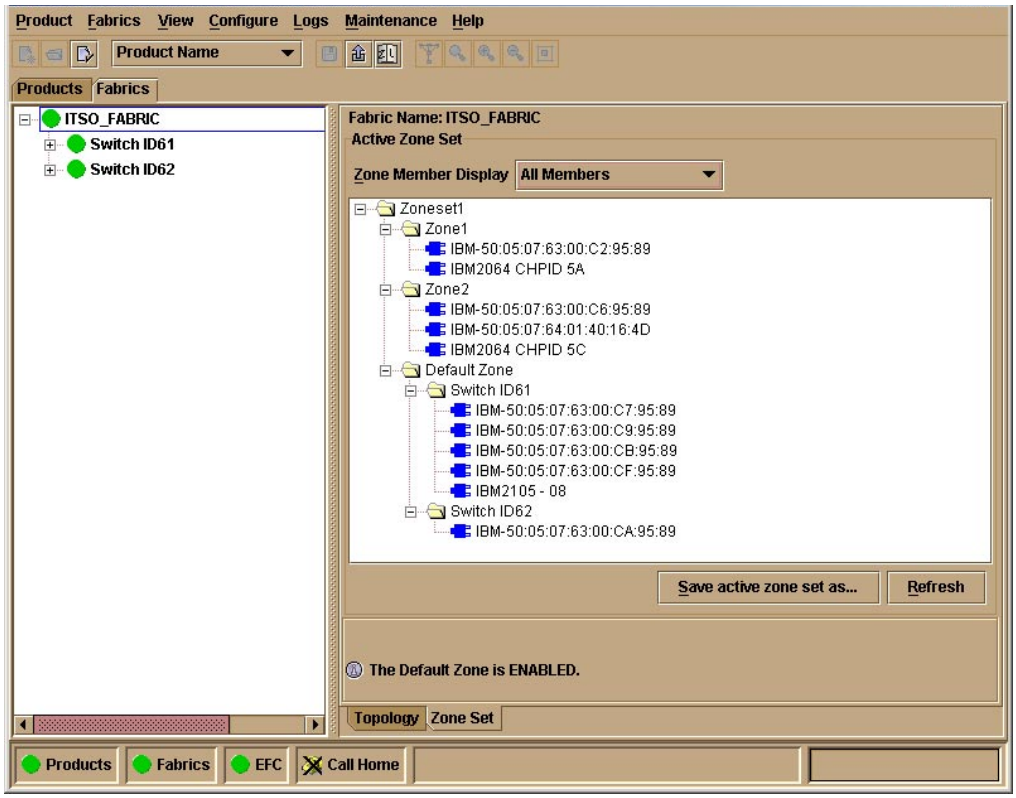


Figure 5-29 Current active zone set and zone members

Compare the listed devices with your configuration documentation (worksheet). If everything is correct you can save these zone settings in a new zone set by clicking **Save Active Zone Set as...** and entering a new name for the current zoneset. This zone set is added to the zone library.

To save defined zones and zonesets go to the Zoning Library, select from the menu bar **File - Export Zone Sets...** On the next panel select a **subDirectory** on the EFC Manager workstation to store the export file, and enter a file name.

From the File menu in the Zoning Library there is also an Import Zone Set.. function available, which allows you to import a zoneset file previously saved.

5.7 Verifying and backing up the configuration

You should have finished the following installation and configuration steps in this chapter:

- Enter Director Domain ID
- Connect ISLs to build a fabric
- Select S/390 operation mode
- Enable Control Unit Port (CUP)
- Enable High Integrity Feature
- Add Directors to membership list
- Enable fabric binding
- Enable Switch Binding
- Configure ports
- Define port names and block ports
- Define Zones and zone sets
- Add ports to zones
- Activate zone set

The current configuration information should be saved and printed. Some export options are available to export configuration data into a file on the EFC Manager workstation:

- Export Configuration Report for each Director
- Export Logs for each Director
- Export Fabric Topology for each fabric
- Export Zone Set for each fabric
- Export Logs for each fabric

Check logs for all Directors and fabrics for any unresolved error occurred during installation and configuration tasks. It there are any errors they should be fixed now.

Export Fabric topology for each fabric. Select *Fabrics - Export Fabric Topology...* from the menu bar. In the next displayed window select the subDirectory where the file should be stored and type a file name. Click **Save** to start the export function. The data are stored in XML format and can be viewed by any editor program as shown in Figure 5-30.

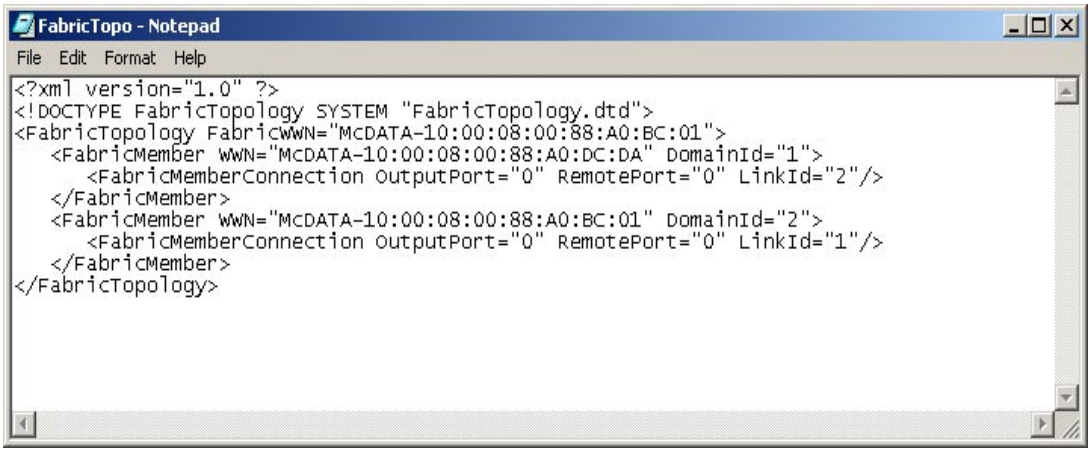


Figure 5-30 Fabric Topology export file view (xml format)

Export zone set for each fabric. Open the Zoning Library window and select File - Export **Zone Set...** from the menu bar. In the next displayed window select the **subDirectory** where the file should be stored and type in a file name. Click **Export**. The data are stored in XML format and can be viewed by any editor program, as shown in Figure 5-31.

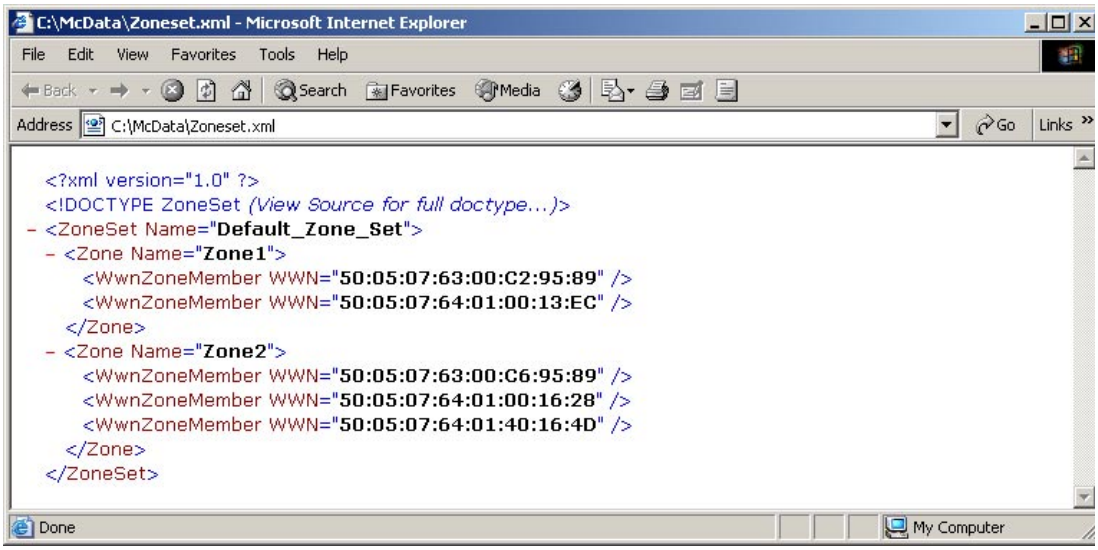


Figure 5-31 Zone Set export file display (xml format)

Export and print the Configuration report for each switch. Select **Configure - Export Configuration Report...** from the menu bar. In the next displayed window select the **subDirectory** where the file should be stored and type in a filename. Click **Save**. The data is stored in txt format and can be viewed by any editor program, as shown in Figure 5-32.

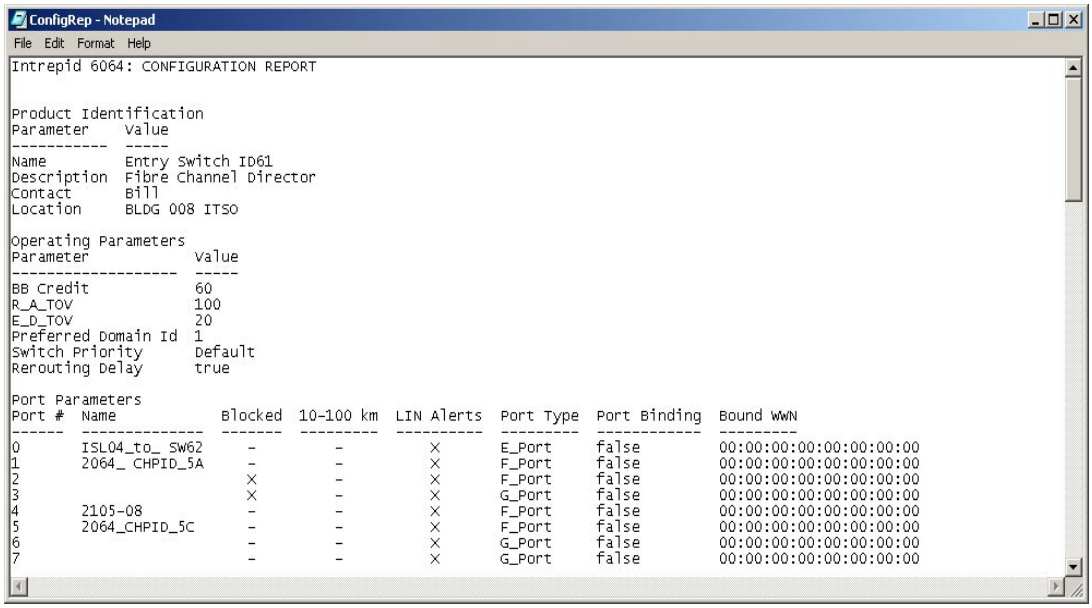

ConfigRep - Notepad
File Edit Format Help
Intrepid 6064: CONFIGURATION REPORT
Product Identification
Parameter Value
Name Entry Switch ID61
Description Fibre Channel Director
Contact Bill
Location BLDG 008 ITSO
Operating Parameters
Parameter Value
BB Credit 60
R_A_TOV 100
E_D_TOV 20
Preferred Domain Id 1
Switch Priority Default
Rerouting Delay true
Port Parameters
Port # Name Blocked 10-100 km LIN Alerts Port Type Port Binding Bound WWN
0 ISL04_to_ SW62 - - X E_Port false 00:00:00:00:00:00:00:00
1 2064_ CHPID_5A - - X F_Port false 00:00:00:00:00:00:00:00
2 X - X F_Port false 00:00:00:00:00:00:00:00
3 X - X G_Port false 00:00:00:00:00:00:00:00
4 2105-08 - - X F_Port false 00:00:00:00:00:00:00:00
5 2064_CHPID_5C - - X F_Port false 00:00:00:00:00:00:00:00
6 - - X G_Port false 00:00:00:00:00:00:00:00
7 - - X G_Port false 00:00:00:00:00:00:00:00

Figure 5-32 Configuration Report export file view (txt format)

The Configuration Report contains the following configuration parameter:

- Product Identification
- Operating Parameters
- Port Parameters
- SNMP Parameters
- Active Zoning Configuration

Print this file and compare the configuration parameter for the fabric, Directors and ports with the configuration data in your worksheet.

Back up of your configuration data. On each Director select *Maintenance - Backup & Restore Configuration* from the menu bar. Click Backup on next panel. The configuration data for the Director is saved on the EFC Server.

A

Useful procedures

This appendix provides procedures needed to supplement configuration tasks described in this document.

In subsequent sections, you will find the following:

- Setting up a HyperTerminal Session
- Altering the IP address of a CTP card
- Installing EFC Management software

© Copyright IBM Corp. 2003. All rights reserved.

Setting up a HyperTerminal session

For some special functions in the McDATA Intrepid FICON Director, it is required to set up a HyperTerminal session. The communication is established via the Maintenance Connector on the rear of the director and a COM port in the workstation PC.

1. Select **Start -> Programs -> Accessories -> HyperTerminal** from your desktop (see Figure A-1).

Figure A-1 HyperTerminal connection description

2. Enter a name (such as Intrepid) in the name field, select an icon and click **OK**. The Connect To window appears (see Figure A-2).

Figure A-2 HyperTerminal Connect to panel

3. Select **COM1** and click **OK**. Ensure the null modem cable is connected to this port. The Port Settings window is displayed.

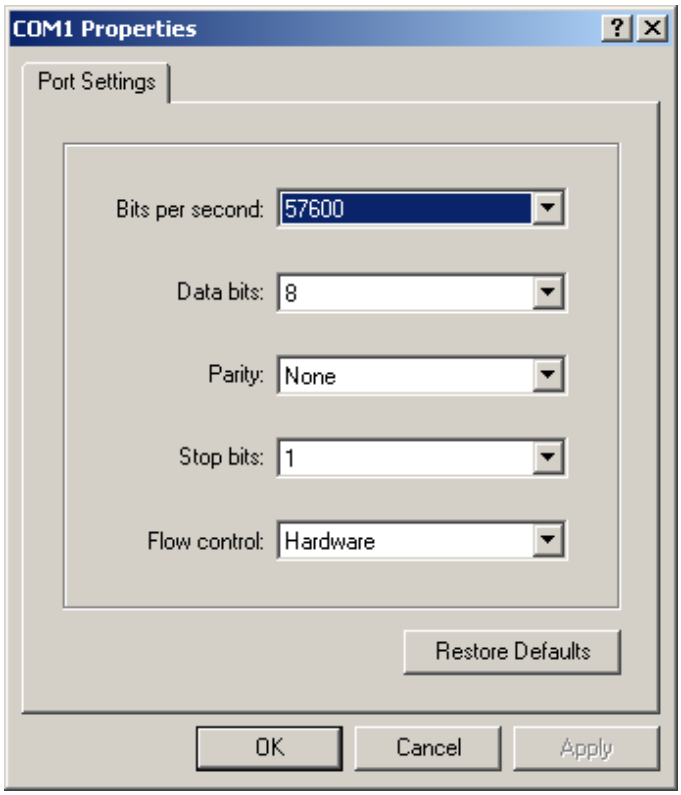


Figure A-3 COM1 properties panel

4. On the COM1 properties screen set the following parameters:
   - Bits per second: 57600
   - Data Bits: 8
   - Parity: None
   - Stop Bits: 1
   - Flow control: Hardware
5. Press Enter until the prompt > appears. Type in the password to establish the terminal session and to execute other commands.

   Password to be entered: `password`

A typical log from a HyperTerminal session is shown in Figure A-4.

```
>xxxxxxxx
C>ipconfig
MAC Address:    08 00 88 A0 DC DA
IP Address:     10.1.8.8
Subnet Mask:    255.255.0.0
Gateway Address: 0.0.0.0

C>help ipconfig

[] = optional   | = or       ^   = optional space
() = required   + = and/or    ... = repetition

IPCONFIG Configure IP parameters: [ <ipAddress> [ <ipMask> [ <ipGateway> ] ] ]

C>ipconfig 10.1.8.2 255.0.0.0 0.0.0.0
```

```
Request Completed: OK

C>ipconfig
MAC Address:    08 00 88 A0 DC DA
IP Address:     10.1.8.2
Subnet Mask:    255.0.0.0
Gateway Address: 0.0.0.0

C>exit
>
```

Figure A-4 HyperTerminal session

Altering an IP address in a CTP card

There are no restrictions for the IP address range used for the McDATA Intrepid. To change an IP address, the following steps must be performed:

1. If the HyperTerminal window is displayed, press Enter and type in the password as described under “Setting up a HyperTerminal session” on page 72.
2. Type in the command **`ipconfig`** to display the current settings.
3. If changes are necessary, type in **`ipconfig ,`**and then separated by a blank, type in the new IP address.

   If more than one parameter has to be changed, you can enter the values in one string, but each field has to be separated by a blank.
4. Entering the command **`ipconfig`** again displays the new value to verify the setting is correct.
5. To terminate the session, type **`exit.`**

Installing EFC Manager server software

This section describes how to install the EFC Manager server application on a workstation. In the EFC Manager server workstation both the server and the client component of the application have to be installed. On all other workstations, it is recommended to install only the client component of the application:

1. On the PC you want to install the EFC Server, exit and close all applications.
2. Run the McDATA server installation.exe file from the CD-ROM you received with the new EFC Management Server version. This installs both the client and server components.
3. After clicking **Next** the License Agreement screen opens. Click the radio button to accept.
4. Read Important Information before you continue with the installation.
5. If you have made your decision related to the shortcut folder, the installation will start.

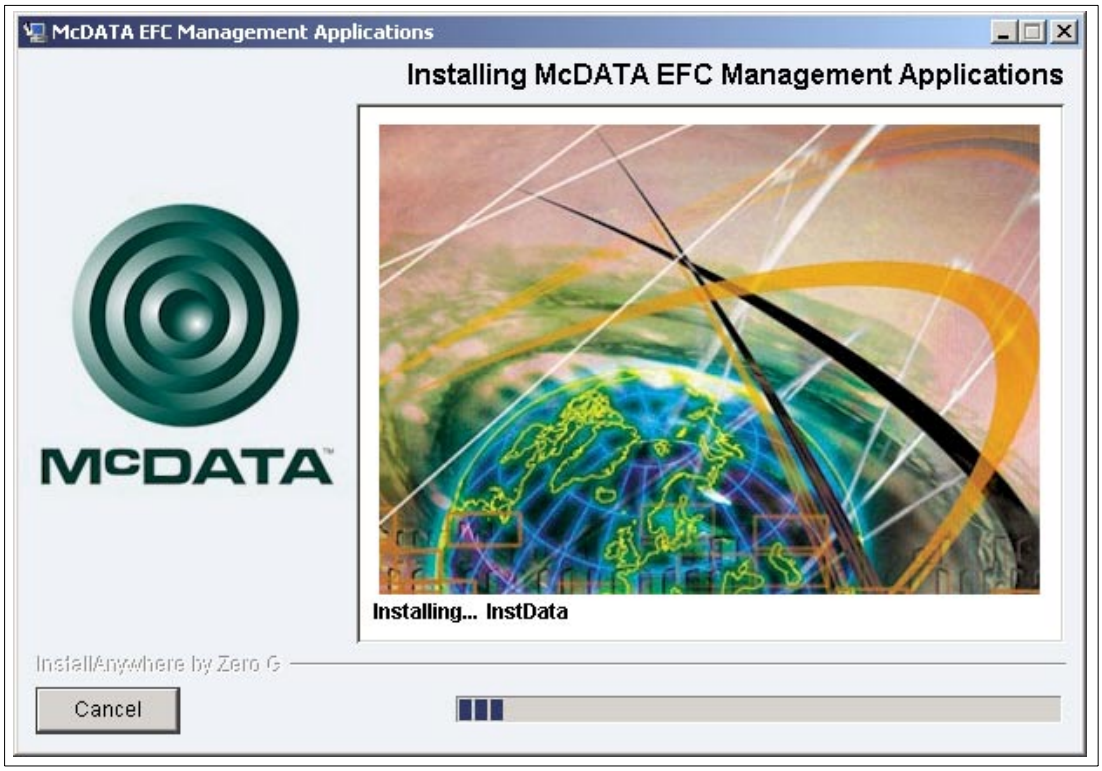


Figure A-5 Installation of the EFC Management Software

After the installation has finished, there will be two more icons on the PCs desktop.

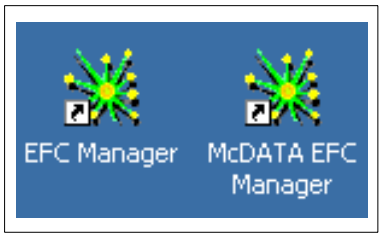


Figure A-6 EFC desktop icons

Installing EFC Management client software

To install the EFC Management client application on a workstation, do the following:

1. Open a browser, and enter the host name or IP address of your EFC Manager server. The McDATA Enterprise Fabric Connectivity Management page appears as shown in Figure A-7.
2. To install the client software, follow the instructions supplied in this page for your workstation platform.

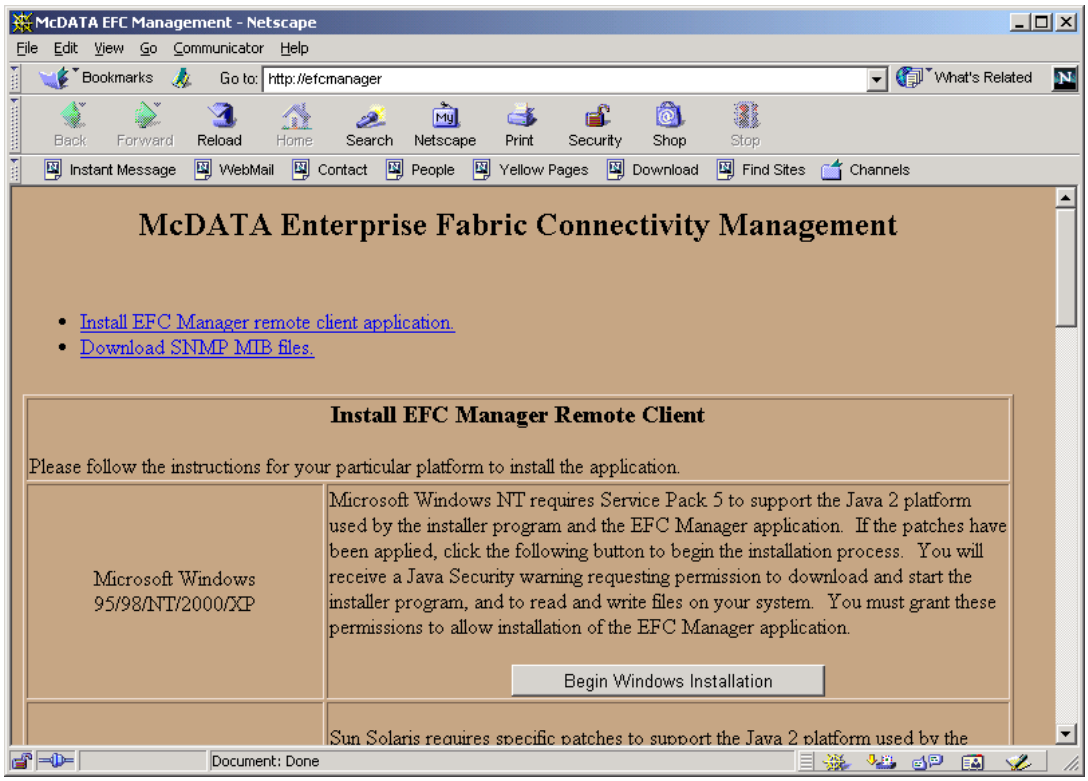

McDATA EFC Management - Netscape
File Edit View Go Communicator Help
Bookmarks Go to: http://efcmanager
What's Related
Back Forward Reload Home Search Netscape Print Security Shop Stop
Instant Message WebMail Contact People Yellow Pages Download Find Sites Channels
McDATA Enterprise Fabric Connectivity Management
Install EFC Manager remote client application.
Download SNMP MIB files.
Install EFC Manager Remote Client
Please follow the instructions for your particular platform to install the application.
Microsoft Windows 95/98/NT/2000/XP
Microsoft Windows NT requires Service Pack 5 to support the Java 2 platform used by the installer program and the EFC Manager application. If the patches have been applied, click the following button to begin the installation process. You will receive a Java Security warning requesting permission to download and start the installer program, and to read and write files on your system. You must grant these permissions to allow installation of the EFC Manager application.
Begin Windows Installation
Sun Solaris requires specific patches to support the Java 2 platform used by the
Document: Done

Figure A-7 Installing EFC Manager client

Upgrading Director firmware

You can download the latest firmware for the Intrepid models from the McDATA home page (http://www.mcdata.com). The upgrade can then be performed from the workstation where the file is stored, by doing the following:

1. Log into the EFC manager, and select the **Director** you want to upgrade.
2. Click the **Firmware Library from the Maintenance** menu on the menu bar, then click **New** (see Figure A-8).

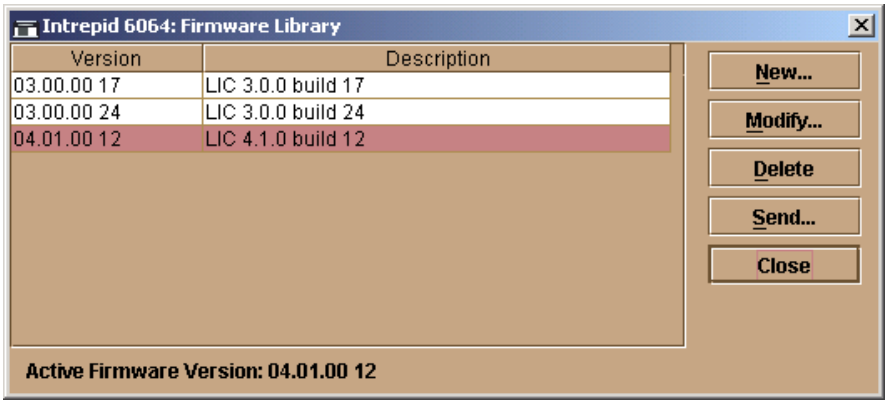


Figure A-8 New firmware version

The New Firmware Version dialog box appears.

3. Select the **appropriate file** from its storage location and click **New.**
4. When the New Firmware Description dialog box displays, enter a description for the new firmware and click **OK**.

> **Note:** Use a date or some other text that identifies the new firmware. The Firmware Library dialog box displays with the version and description of the new firmware added to the text area.

5. After the new firmware version is loaded, select it in the **New Firmware Version** dialog box, then click **Send**.
6. When the warning box displays to confirm sending the firmware, click **Yes** to proceed.

B

Port location and mapping

This appendix provides information about the physical layout of McDATA Intrepid FICON Director models. These models allow for a wide range of configuration options. The basic building block is the port module, which contains four Fibre Channel/FICON ports using 1 Gbps and/or 2 Gbps technology. For more configuration details go to 2.1.4, “Hardware components” on page 15.

In the subsequent sections, you will find diagrams depicting the following:

- Port mapping of the Intrepid 6064
- Port mapping of the Intrepid 6140

© Copyright IBM Corp. 2003. All rights reserved.

Intrepid port numbering

For the Intrepid (6064 and 6140) FICON Directors, the *physical port numbers* are the same as the *port addresses*. The Hardware Configuration Definition (HCD) and Input Output Configuration Program (IOCP) use port address information to define control unit link addresses. The physical port number is indicated either by a decimal or hexadecimal value, which can be found in the ECF Manager logs as identification for a given port. See Figure B-1 for physical port number and port address mapping information.

Note: A port number may have a different port address assigned if a port swap was performed.

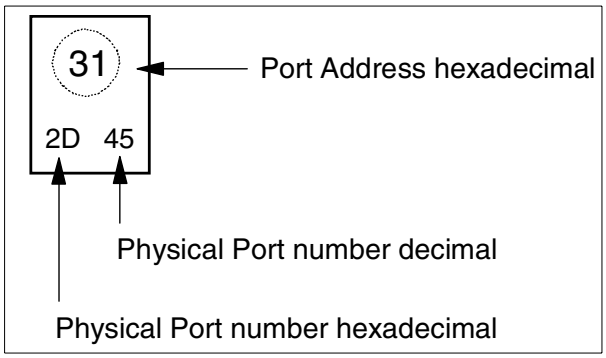


Figure B-1 Port numbering

This example shows a decimal port number of 45 (x'2D') and the port address is 31, which is the address used for HCD and IOCP definitions.

Intrepid 6064 port address mapping

Figure B-2 on page 81 shows the port layout for Intrepid 64-port FICON Director with the assigned port ranges. Port numbering starts at the left, and continues to the right of the Director. Notice that the counting of ports starts in slot 0 from the bottom of the card.

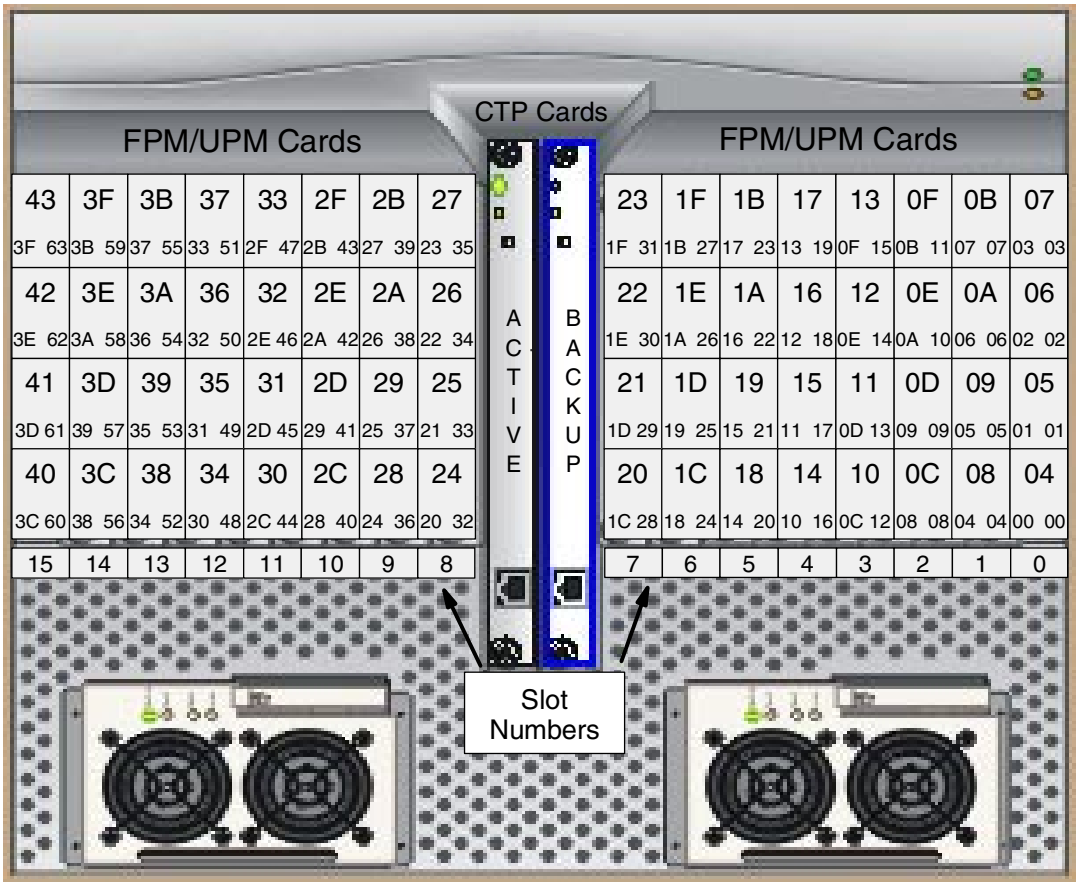


Figure B-2 Port mapping for the Intrepid FICON Director

Intrepid 6140 port address mapping

Figure B-3 on page 82 shows the port layout for Intrepid 140-port FICON Director with the assigned port ranges. Notice that on this Director, there are 128 ports in the front. The remaining 12 ports are available in the rear.

In a cascaded FICON topology, it is recommended to use the rear ports for the Inter-Switch Links.

Port numbering starts at the left lower part of the Director, continuing to the right lower part, and then to the upper left part through the upper right part.

Notice that the counting of ports starts in slot 0 from the top of the card.

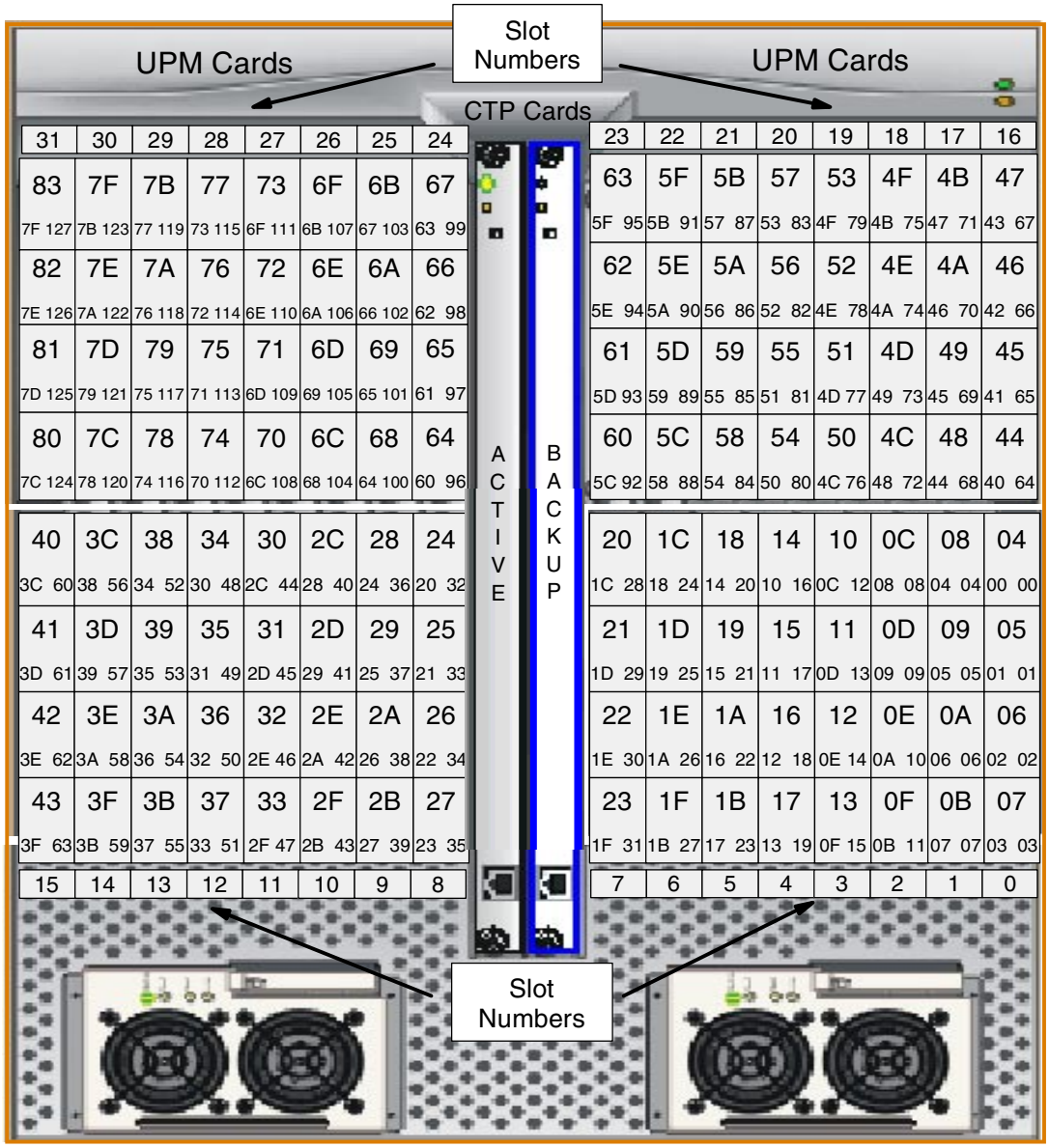


Figure B-3 Port Mapping for the Intrepid 6140 FICON Director

The remaining 12 ports in the rear are identified as shown in Figure B-4.

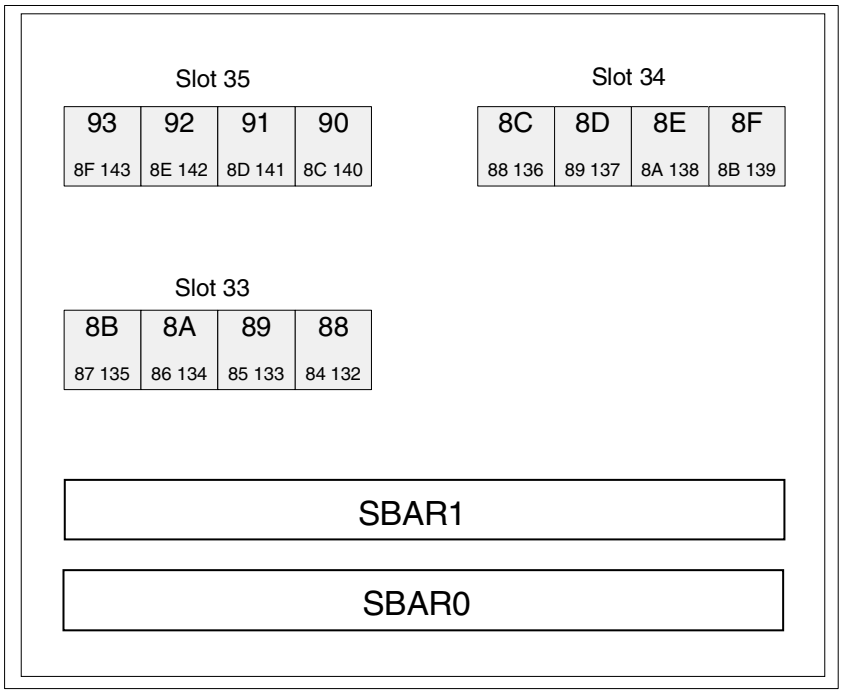


Figure B-4 Intrepid 6140 rear port mapping

C

FICON Director configuration worksheet

This appendix contains a worksheet, which aids in documenting the layout of your FICON Director. It can be applied as a tool to help understand how the ports are allocated for configuration and problem determination purposes.

© Copyright IBM Corp. 2003. All rights reserved.

FICON Director Configuration Worksheet

FICON Director Manufacturer: _____ Type: _____ Model: ____ S/N _____

HCD defined Switch ID _____ (Switch ID)
FICON Director Domain ID _____ (Switch @)

Cascaded Directors No ___ Yes ___
Corresponding cascaded Director Domain ID _____
Fabric name _____

FICON Director Ports					Attached N_Ports / E_Ports (CU, CPC or ISL)				
Slot Number	Port Number	Port Address	Laser Type: LX / SX	Port Name	Node Type CU / CHNL	Machine Type	Model	Serial Number	ISL CU I/F CPC CHPID

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

IBM Redbooks

For information on ordering these publications, see “How to get IBM Redbooks” on page 87.

- *FICON Native Implementation and Reference Guide,* SG24-6266

Other resources

These publications are also relevant as further information sources:

- *McDATA Enterprise Fabric Connectivity Manager,* 620-005001-600
- *McDATA Products in a SAN Environment Planning Manual,* 620-000124-000
- *McDATA Intrepid 6064 Director Installation and Service Manual*, 620-000108-500
- *McDATA SNMP Support Manual*, 620-000131-200
- *McDATA Intrepid 6064 Director Product Manager User Manual,* 620-000120-200

Referenced Web sites

These Web sites are also relevant as further information sources:

- McDATA Intrepid documentation and information

  http://www.mcdata.com/ibm

- IBM offerings for McDATA Intrepid

  http://http://www.ibm.com/storage/mcdata

How to get IBM Redbooks

You can order hardcopy Redbooks, as well as view, download, or search for Redbooks at the following Web site:

ibm.com/redbooks

You can also download additional materials (code samples or diskette/CD-ROM images) from that site.

IBM Redbooks collections

Redbooks are also available on CD-ROMs. Click the CD-ROMs button on the Redbooks Web site for information about all the CD-ROMs offered, as well as updates and formats.

© Copyright IBM Corp. 2003. All rights reserved.

Index

A
arbitrated loop 6
architecture
  website 5
Audit log 42
auto-negotiate 3

B
Backplane 17
BB_Credit 52
Bound WWN 28

C
communication methods 13
Control Processor (CTP) 15
Control Unit Port (CUP) 50
conversion kit 22, 32
CTP 36
CTP cards 23

D
definition terms 25
Director characteristics 12
Director configuration
  Intrepid 6064 17
  Intrepid 6140 17
Domain ID 25, 55

E
E_D_TOV 52
E_Port 2
EFC Manager
  software installation 75
EFC Server 14
Enterprise Fabric mode 54
Event log 42
export 69
export zoneset 68

F
F_Port 2
fabric binding 9, 29
Fabric log 42
fabric membership 55
Fabrics view 40
Fan Module 17
FC link 2
  data rate 3
FC-1 level 5
FC-2 level 5
FC-3 level 5
FC-FCP 5
FC-FG
  architecture 5
FC-FS
  architecture 4
FC-PH 5
  amendments 5
  architecture 5
FC-SB-2 5
FC-SW 5
  architecture 5
Feature Code 6003 19
Feature Code 6006 18
Feature Code 6007 18
Feature Code 6302 19
feature codes
  FICON 32
  FICON Express 32
Fiber Port Module (FPM) 15
Fibre Channel
  framing and signalling 4
Fibre Channel (FC) protocols 4
FICON
  channel 4
  CU characteristics 34
  distances 33
FICON channel
  topologies 6
FICON channel mode
  bridged (FCV) 5
  Fibre Channel Protocol (FCP) 6
  native (FC) 5
FICON Management Server 19
FICON SANtegrity 18
firmware 76
firmware version 13, 37
FPM cards 23

G
G_Port 2

H
High integrity 9
high integrity fabric 9
high-availabiltiy features 18
HIPPI 5
HyperTerminal 36, 72

I
initial program load (IML) 15
Insistent 48
Insistent Domain IDs 28
Insistent domain IDs 9

© Copyright IBM Corp. 2003. All rights reserved.

interconnection 13
Interop Mode 52
Inter-Switch Link (ISL) 22
IP address 23, 36
IPI 5
ISL 23

L
link attenuation 33
link budget 33
LINK keyword 26
long distance buffering 61
Long wavelength (LX) 12
long wavelength (LX) 32

M
Management Server Function 50
membership list 28, 57
Mode Conditioning Patch (MCP) 22
mode conditioning patch (MCP) 32
multimode 33

N
Network Address option 37
network configuration 23
New Product panel 37
nickname 59
Node 2

O
occupied 28
offline state 46
offset 25

P
Parallel Access Volumes (PAV) 34
physical port numbers 80
Port 2
port address 26
port addresses 80
port binding 28, 61
port layout 80–81
Power Module Assembly 16
Power Supply 16
preferred Domain ID 48
Product Managers 13
Products view 38
prohibit 60
protocol intermix 12

Q
Query Security Attributes 19

R
R_A_TOV 52
receiver 4
Redbooks Web site 87
  Contact us viii
redundancy 12
RFI shield 16

S
S/390 Operating Mode 48
SANtegrity 48
SBAR Assembly 17
SBCON 5
SCSI 5
service LAN 23, 37
short wavelength (SX) 12, 32
single mode 33
small form factor (SFF) 12
Speed 48
supported distances 33
switch address range 25
switch binding 29
Switch ID range 25
SWITCH keyword 26
Switched fabric 2

T
Topology view 41
transmission
  media 4
transmitter 4

U
Universal Port Module (UPM) 15
UPM cards 23
User options 41

W
worksheet 85
World-Wide Names (WWN) 3
World-Wide Node_Name (WWNN) 3
World-Wide Port_Name (WWPN) 3

Z
zone set 64–65
zoning 61
zoning library 62, 65

IBM Redbooks

Getting Started with the McDATA Intrepid FICON Director

(0.2”spine)
0.17”<->0.473”
90<->249 pages

Getting Started with the McDATA Intrepid FICON Director

Product, planning, and implementation information

Realistic considerations and suggestions

Helpful configuration examples

This IBM Redbook discusses how to install, tailor, and configure the McDATA Intrepid FICON Director, in conjunction with the FICON topologies supported by zSeries and 9672 Generation 5 and Generation 6 servers. It focuses on the hardware installation as well as the software definitions needed to provide connectivity for supported FICON environments.

This redbook provides planning information and FICON Director setup information. Also included are helpful utilities for monitoring and managing the McDATA Intrepid FICON Director environment.

This book is intended for system engineers, SAN administrators, and system programmers who will plan and install McDATA Intrepid FICON Directors. A good background in systems planning, hardware and cabling infrastructure planning, and zSeries I/O definitions (HCD or IOCP), as well as Fibre Channel or FICON Directors is assumed.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-6857-00 ISBN 0738428426